3com

3Com Router

Command Reference Guide Addendum for V1.20

http://www.3com.com/

Part No. 10014302
Published January 2004

1.1. Introduction

1.1.1. Scope

This manual provides command reference information for new software features found in V1.20 of the 3Com Router operating system. Use this addendum to supplement command reference information found in the *3Com Router Command Reference Guide*.

1.1.2. Online Resources

Download the *Router 3000 Installation Guide* from:
http://support.3com.com/infodeli/tools/routers/R3000Install.pdf
Download the *Router 5000 Installation Guide* from:
http://support.3com.com/infodeli/tools/routers/5000Install.pdf
Download the *3Com Router Command Reference Guide* from:
http://support.3com.com/infodeli/tools/routers/3ComRouterComRef.pdf
Download the *3Com Router Configuration Guide* from:
http://support.3com.com/infodeli/tools/routers/3com_configuration_guide.pdf
Download other current software updates and release notes from:
http://www.3com.com/

Chapter 1 CBQ Configuration Commands

1.1 af

Syntax

af bandwidth { *bandwidth* | **pct** *percentage* }

undo af

View

Policy-class view

Parameter

bandwidth: Bandwidth in kbit/s in the range of 8 to 1000000.

percentage: Percentage of available bandwidth in the range of 1 to 100.

Description

Using the **af** command, you can configure the class to perform the assured-forwarding and the minimum bandwidth used. Using the **undo af** command, you can cancel the configuration.

Both user-defined class and default-class are configurable.

The sum of the bandwidths assigned to the assured-forwarding and expedited-forwarding classes of the same policy must be smaller than the available bandwidth of the interface applied by the policy.

All bandwidth values involved in a policy must be configured as the same type, for example, all in absolute value or percentage form.

For the related command, see **qos policy**, **qos-class**.

Example

Configure the "database" class of the "3Com" policy to perform assured-forwarding with the minimum bandwidth as 200kbit/s.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database] af bandwidth 200
```

1.2 car

Syntax

car cir *rate* [**cbs** *size* **ebs** *size*] [**conform** *action* [**exceed** *action*]]

undo car

View

Policy-class view

Parameter

cir *rate*: Committed information rate in the range of 8000 to 155000000 bit/s.

cbs *size*: Committed burst size, that is, the number of bits that can be sent in each interval in the range of 15000 to 155000000 bits. By default, it is 15000.

ebs *size*: Excessive burst size in the range of 0 to 155000000 bits. By default, it is 0.

Conform: Action (defaulted to **pass**) conducted to the packets when the traffic of the packets conforms to the CIR.

exceed: Action (defaulted to **discard)** conducted to the packets when the traffic of the packets does not conform to the CIR.

action: Action conducted to a packet, including:

- discard: Drop the packet
- remark-dscp-pass new-dscp: Set new-dscp and transmit the packet. It ranges from 0 to 63.
- remark-prec-pass new-precedence: Set new-precedence of IP and transmit the packet. It ranges from 0 to 7.
- pass: Transmit the packet.

Description

Using the **car** command, you can configure traffic monitoring for a class. Using the **undo car** command, you can delete the configuration of traffic monitoring.

When being used in interface policy, **car** can be used in the input or output direction of the interface.

Applying a policy configured with **car** on an interface will cause the previous **qos car** command ineffective.

If this command is frequently configured on the classes of the same policy, the last configuration will overwrite the previous ones.

For the related command, see **qos policy**, **qos-class**.

Example

Configure traffic monitoring for a class. The normal traffic of packets is 38400bit/s. Burst traffic twice of the normal traffic can pass initially and later the traffic is transmitted normally when the rate does not exceed 38400bit/s. When the rate exceeds 38400bit/s, the precedence of the packet turns to 0 and the packet is transmitted.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database] car cir 38400 cbs 76800 ebs 0 conform pass
exceed remark-prec-pass 0
```

1.3 debugging qos

Syntax

debugging qos { { **cbq** { **af** | **be** | **ef** | **class** } } | **cq** | **pq** | **wfq** } [**interface** *type number*]

undo debugging qos { { **cbq** { **af** | **be** | **ef** | **class** } } | **cq** | **pq** | **wfq** } [**interface** *type number*]

View

All views

Parameter

cbq af: Enable the debugging of confirming forwarding information in CBQ.

cbq be: Enable the debugging of best-effort forwarding information in CBQ.

cbq ef: Enable the debugging expedited-forwarding information in CBQ.

cbq class: Enable the debugging of the class information of CBQ.

cq: Enable the debugging of the CQ.

pq: Enable the debugging of the PQ.

wfq: Enable the debugging of the WFQ.

interface *type number*: Enable the debugging of the interface QoS. If this parameter is not used, the QoS debugging of all interfaces will be enabled.

Description

Using the **debugging qos** command, you can enable the debugging of QoS. Using the **undo debugging qos** command, you can disable the debugging of Qos.

By default, the debugging of QoS is disabled.

Example

Enable the debugging of the CBQ class information on the interface Serial0.

```
[Router] debugging qos cbq class interface serial 0
```

1.4 display qos cbq interface

Syntax

display qos cbq interface [*type number*]

View

All views

Parameter

interface-type: Interface type.

number: Interface number.

Description

Using the **display qos cbq interface** command, you can browse the class-based queue configuration information and running status of the specified interface or all interfaces.

Example

```
[3Com] display qos cbq interface
Interface: Ethernet0
Class Based Queueinging: (Output queue: Total Size/Discards)
  CBQ:  0/0
  Queue Size:  0/0/0 (EF/AF/BE)
  BE Queues:   0/0/256 (Active/Max active/Total)
  AF Queues:   1 (Allocated)
  Bandwidth(Kbps): 74992/75000 (Available/Max reserve)
```

1.5 display qos class

Syntax

display qos class [*class-name*]

View

All views

Parameter

class-name: Name of the class. By default, the information of all classes are displayed.

Description

Using the **display qos class** command, you can browse the class information concerning router configuration.

Example

```
[3Com] display qos class
QoS Class Configuration Information:
  Class: 3COM
   Operator: Logical AND
   Rules: If-match ip-precedence 5

  Class: database
   Operator: Logical AND
   Rules: If-match ACL 131
       If-match inbound-interface Ethernet0
```

1.6 display qos policy

Syntax

display qos policy [*policy-name* [**class** *class-name*]]

View

All views

Parameter

policy-name: Name of policy. By default, the configuration information of all policies are displayed.

class-name: Class name in the policy.

Description

Using the **display qos policy** command, you can browse the configuration information of the specified or all classes of the specified or all policies.

Example

```
[3Com] display qos policy
  QoS Policy Configuration Information:
  Policy: test

   Class: default-class
    Behavior(s):
      -none-

   Class: AF
    Behavior(s):
      Committed Access Rate:
         CIR 8000 (Bps), CBS 15000 (Bit), EBS 0 (Bit)
         Conform Action: pass
         Exceed Action: discard

  Policy: 3Com

   Class: default-class
    Behavior(s):
      -none-

   Class: 3COM
    Behavior(s):
       Expedited Forwarding
       Bandwidth 8 (Kbps) Burst 1500 (Byte)

   Class: AF
    Behavior(s):
       Assured Forwarding
       Bandwidth 20 (%)
       Discard Method: Tail (Max Threshold 64 packets)
```

```
    Committed Access Rate:
     CIR 8000 (Bps), CBS15000 (Bit), EBS 0 (Bit)
     Conform Action: remark mpls exp 3 and pass
     Exceed Action:  discard

  Class: SHAPE
   Behavior(s):
     Traffic Shape:
      CIR 8000 (Bps), CBS 15000 (Bit), EBS 0 (Bit)
      Queue Length 1024 (Packet)
```

1.7 display qos policy interface

Syntax

display qos policy interface [{ *type number* } [**inbound** | **outbound**]

View

All views

Parameter

interface-type: Interface type.

number: Interface number.

Description

Using the **display qos policy interface** command, you can view configuration information and operating status of the policy on the specified interface, the specified PVC on specified ATM interface or on all interfaces and PVC.

Example

```
[3Com] display qos policy interface Ethernet 0
  Interface: Ethernet10
  Direction: Outbound

  Policy: 3Com

   Class: default-class
    Matched:  0/0 (Packets/Bytes)
    Rule(s): If-match any
```

```
 Behavior(s):
 Default Queue:
   Flow Based Fair Queueing
     Max number of hashed queues 256
     Matched:  0/0 (Packets/Bytes)
     Enqueued: 0/0 (Packets/Bytes)
     Discarded:  0/0 (Packets/Bytes)
     Discard Method: Tail

Class: 3COM
 Matched:  0/0 (Packets/Bytes)
 Operator: Logical AND
 Rule(s): If-match ip-precedence 5
 Behavior(s):
   Expedited Forwarding
     Bandwidth 8 (Kbps), Burst 1500 (Byte)
     Matched:   0/0 (Packets/Bytes)
     Enqueued:  0/0 (Packets/Bytes)
     Discarded:  0/0 (Packets/Bytes)

Class: AF
 Matched:  0/0 (Packets/Bytes)
 Operator: Logical AND
 Rule(s): If-match ACL 131
      If-match ACL 101
      If-match inbound interface Ethernet0
 Behavior(s):
   Traffic Police:
     CIR 8000 (bps), CBS 15000 (bit), EBS 0 (bit)
     Conform Action: remark mpls exp 3 and pass
     Exceed Action:  discard
     Conformed: 0/0 (Packets/Bytes)
     Exceeded:  0/0 (Packets/Bytes)
   Assured Forwarding
     Bandwidth 14998 (Kbps)
     Matched:  0/0 (Packets/Bytes)
     Enqueued: 0/0 (Packets/Bytes)
     Discarded:  0/0 (Packets/Bytes)
Class: SHAPE
 Matched:  0/0 (Packets/Bytes)
 Operator: Logical AND
 Rule(s): -none-
   Behavior(s):
```

```
    General Traffic Shaping:
      CIR 8000 (Bps), CBS 15000 (Bit), EBS 0 (Bit)
      Queue Length: 1024 (Packets)
      Queue Size:  0 (Packets)
      Pass   :  0/0 (Packets/Bytes)
      Discard :  0/0 (Packets/Bytes)
      Delay  :  0/0 (Packets/Bytes)

  Interface: Serial0
  Direction: Inbound

  Policy: test

   Class: default-class
    Matched:  0/0 (Packets/Bytes)
    Rule(s): If-match any

    Behavior(s):
      -none-

   Class: AF
    Matched:  0/0 (Packets/Bytes)
    Operator: Logical AND
    Rule(s):  If-match ACL 13
           If-match ACL 101
           If-match inbound interface Ethernet0
    Behavior(s):
      Committed Access Rate:
        CIR 8000 (Bps), CBS 15000 (Bit), EBS 0 (Bit)
        Conform Action: pass
        Exceed Action:  discard
        Conformed: 0/0 (Packets/Bytes)
        Exceeded:  0/0 (Packets/Bytes)
```

1.8 ef

Syntax

ef bandwidth *bandwidth* [**cbs** *size*]

undo ef

View

Policy-class view

Parameter

bandwidth: Bandwidth in kbit/s in the range of 8 to 1000000.

size: Specify the allowed burst size in byte in the range of 32 to 2000000. By default, it is bandwidth * 25.

Description

Using the **ef** command, you can configure certain class to perform expedited-forwarding to send the packets of this class into priority queue and configure its maximum bandwidth. Using the **undo ef** command, you can remove the configuration.

The command can not be used together with **queue af**, **queue-length** and **wred** in class view.

This command is unavailable for default-class.

For the related command, see **qos policy**, **qos-class**.

Example

Configure the packets of this class to enter the priority queue, the maximum bandwidth as 200kbit/s and the default burst size as 5000 bytes.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database] ef bandwidth 200 cbs 5000
```

1.9 gts

Syntax

gts cir *rate* [**cbs** *size* [**ebs** *size* [**queue-length** *length*]]]

undo gts

View

Policy-class view

Parameter

cir *rate*: Committed information rate.

cbs *size*: Burst size in the range of 15000 to 155000000 bits. By default, it is equal to half of **cir** *rate*.

ebs *size*: Excessive burst size in the range of 0 to 155000000 bits. By default, it is 0.

queue-length *length*: Queue length in the range of 1 to 1024. By default, it is 50.

Description

Using the **gts** command, you can configure traffic shaping for a class. Using the **undo gts** command, you can delete traffic shaping for a class.

The policy configured with **gts** can only be applied to the output direction of an interface.

Applying a policy configured with **gts** on an interface will cause the previously configured **qos gts** command ineffective.

If this command is frequently configured on classes of the same policy, the last configuration will overwrite the previous ones.

For the related command, see **qos policy**, **qos-class**.

Example

Configure GTS for a class with the specific features as follows: the normal traffic is 38400bit/s; the burst traffic twice normal traffic can pass initially; the traffic no larger than 38400bit/s can be transmitted normally under normal conditions and that larger than 38400bit/s enters queue buffer lately; the buffer queue length is 100.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database] gts cir 38400 cbs 76800 ebs 0 queue-length
100
```

1.10 if-match acl

Syntax

if-match [**logic-not**] **acl** *acl-number*

undo if-match [**logic-not**] **acl** *acl-number*

View

Class view

Parameter

access-list-number: ACL number.

logic-not: Do not match the class.

Description

Using the **if-match acl** command, you can define an ACL match rule. Using the **undo if-match acl** command, you can delete an ACL match rule.

For the related command, see **qos class**.

Example

Define a class to match ACL101.

```
[3Com] qos class class1
[3Com-qosclass-class1] if-match acl 101
```

1.11 if-match any

Syntax

if-match [**logic-not**] **any**

undo if-match [**logic-not**] **any**

View

Class view

Parameter

logic-not: Do not match the class.

Description

Using the **if-match any** command, you can define the match rule for all packets. Using the **undo if-match any** command, you can delete the match rule for all packets.

For the related command, see **qos class**.

Example

Define match rule for all packets.

```
[3Com] qos class class1
[3Com-qosclass-class1] if-match any
```

1.12 if-match class

Syntax

if-match [**logic-not**] **class** *class-name*

undo if-match [**logic-not**] **class** *class-name*

View

Class view

Parameter

class-name: Class name.

Description

Using the **if-match class** command, you can define the match rule for a QoS class. Using the **undo if-match class** command, you can delete the match rule for the QoS class.

This configuration method is the only one to match the traffic with both the match-all and match-any features.

For example: define classA to fit into the following relations: rule1 & rule2 | rule3

qos class logic-and classB

if-match rule1

if-match rule2

qos class logic-or classA

if-match rule3

if-match classB

For the related command, see **qos class**.

Example

Define class2 by invoking class1.

Define match rule for class2. As class1 will be invoked, you should configure class1 first.The match rule for class1 is: IP precedence is 5.

```
[3Com] qos class class1
[3Com-qosclass-class1] if-match ip-precedence 5
```

Define class2 packets with the match rule as class1 and destination MAC address as 0050-BA27-BED3.

```
[3Com] qos class class2
[3Com-qosclass-class2] if-match class class1
[3Com-qosclass-class2] if-match destination-mac 00-50-BA-27-BE-D3
```

1.13 if-match *criteria*

Syntax

if-match [**logic-not**] *criteria*

undo if-match [**logic-not**] *criteria*

View

Class view

Parameter

criteria: Match rule of a class, which can be **acl**, **any**, **class-map**, **destination-mac**, **inbound-interface**, **ip-precedence**, **dscp**, **protocol**, **source-mac** or **mpls-exp**.

Description

Using the **if-match not** command, you can define the rule for all packets not satisfying the specified match rule. Using the **undo if-match not** command, you can delete the rule of all packets not satisfying the specified match rule.

For the related command, see **qos class**.

Example

Define the packets with class match protocol not being IP.

```
[3Com] qos class class1
[3Com-qosclass-class1] if-match logic-not protocol ip
```

1.14 if-match inbound-interface

Syntax

if-match [**logic-not**] **inbound-interface** { *type number* }

undo if-match [**logic-not**] **inbound-interface** { *type number* }

View

Class view

Parameter

interface-type: Interface type.

number: Interface number.

Description

Using the **if-match inbound-interface** command, you can define input interface match rule of a class. Using the **undo if-match inbound-interface** command, you can delete input interface match rule of a class.

When defining a match rule, the specified interface must be existent.

Supported interface types: Ethernet interface, serial interface, Tunnel interface, virtual template interface, etc.

For the related command, see **qos class**.

Example

Define the packets with the class match input interface as Ethernet0.

```
[3Com] qos class class1
[3Com-qosclass-class1] if-match inbound-interface Ethernet 0
```

1.15 if-match ip-dscp

Syntax

if-match [**logic-not**] **ip-dscp** *value* [*value*] …

undo if-match [**logic-not**] **ip-dscp** *value* [*value*] ...

View

Class view

Parameter

ip-dscp *value*: DSCP value in the range of 0 to 63.

Description

Using the **if-match dscp** command, you can define DSCP match rule. Using the **undo if-match dscp** command, you can delete DSCP match rule.

You can configure this command for a class for several times. When a command is configured, the *ip-dscp-value* will be sorted in the ascending order automatically. Only when the specified DSCP values are identical with those in the rule (sequence may be different), can the command be deleted.

Up to 8 DSCP values can be configured by a command. If several DSCPs are configured with the same value, they will considered as one by default. The relation between different DSCP values is “OR”.

For the related command, see **qos class**.

Example

Define the match rule of class1 as matching the packets with the DSCP value as 1, 6 or 9.

```
[3Com] qos class class1
[3Com-qosclass-class1] if-match ip-dscp 1 6 9
```

1.16 if-match ip-precedence

Syntax

if-match [**logic-not**] **ip-precedence** *value* [*value*] …

undo if-match [**logic-not**] **ip-precedence** *value* [*value*] …

View

Class view

Parameter

ip-precedence *value*: IP precedence value in the range of 0 to 7.

Description

Using the **if-match ip-precedence** command, you can define IP precedence match rule. Using the **undo if-match ip-precedence** command, you can delete IP precedence match rule.

When the command is configured, the ip-precedence-value will be sorted automatically in ascending order.

Up to 8 precedence values can be specified. If several identical precedence values are specified, the system regards them as one. The relation between different precedence values is “OR”.

For the related command, see **qos class**.

Example

Define the match rule of class1 as matching the packets with the precedence value as 1 or 6.

```
[3Com] qos class class1
[3Com-qosclass-class1] if-match ip-precedence 1 6
```

1.17 if-match mac-address

Syntax

if-match [**logic-not**] { **destination-mac** | **source-mac** } *mac-address*

undo if-match [**logic-not**] { **destination-mac** | **source-mac** } *mac-address*

View

Class view

Parameter

mac-address: MAC address in the format of xx-xx-xx-xx-xx-xx.

Description

Using the i**f-match** { **destination-mac** | **source-mac** } command, you can define the match rule for destination or source address. Using the **undo if-match** { **destination-mac** | **source-mac** } command, you can delete the match rule for destination or source address.

The match rule for destination MAC address is effective only for output policies and Ethernet interfaces.

The match rule for source MAC address is effective only for input policies and Ethernet interfaces.

For the related command, see **qos class**.

Example

Define the match rule of class1 as follows: match the packets with the destination MAC address as 0050-ba27-bed3.

```
[3Com] qos class class1
[3Com-qosclass-class1] if-match destination-mac 00-50-ba-27-be-d3
```

Define the match rule of class2 as follows: match the packets with source MAC address as 0050-ba27-bed2.

```
[3Com] qos class class2
[3Com-qosclass-class2] if-match source-mac 00-50-ba-27-be-d2
```

1.18 if-match protocol

Syntax

if-match [**logic-not**] **protocol ip**

undo if-match [**logic-not**] **protocol ip**

View

None

Parameter

Class view

Description

Using the **if-match protocol** command, you can define IP match rule. Using the **undo if-match protocol** command, you can delete IP match rule.

For the related command, see **qos class**.

Example

Define the packets whose class match protocol is IP.

```
[3Com] qos class class1
[3Com-qosclass-class1] if-match protocol ip
```

1.19 if-match rtp

Syntax

if-match [**logic-not**] **rtp start-port** *starting-port-number* **end-port** *end-port-number*

undo if-match [**logic-not**] **rtp start-port** *starting-port-number* **end-port** *end-port-number*

View

Class view

Parameter

starting-port-number: Starting RTP port number in the range of 2000 to 65535.

end-port-number: Ending RTP port numbers in the range of 2000 to 65535.

Description

Using the **if-match rtp** command, you can define port match rule of RTP. Using the **undo if-match rtp** command, you can delete the port match rule of RTP.

This command is used to match RTP packets in the specified RTP port range, that is, match the packets of even UDP port numbers between *starting-port-number* and < *end-port-number*. If this command is frequently used under a class, the last configuration will overwrite the previous ones.

For the related command, see **qos class**.

Example

Define the match rule of class1 as matching the packets whose RTP port number is the even UDP port number between 16384 and 32767.

```
[3Com] qos class class1
[3Com-qosclass-class1] if-match rtp start-port 16384 end-port 32767
```

1.20 qmtoken

Syntax

qmtoken *token-number*

undo qmtoken

View

Interface view

Parameter

token-number: The number of sending tokens, in the range from 1 to 50.

Description

Using the **qmtoken** command, you can configure the number of QoS sending tokens. Using the **undo qmtoken** command, you can disable the sending token function of QoS.

By default, disable QoS sending token function.

In such operation as FTP transmission, QoS queue may become invalid since the upper layer provides flow control function. QoS sending token function provides a kind of traffic control mechanism for the lower layer queue, and the number of packets sent to the lower layer interface queue can be controlled according to the number of tokens.

In normal conditions, it is suggested to set the number of sending tokens to 1 during FTP transmission.

Note:

After this command is configured, you need to restart the interface with the shutdown / undo shutdown function. Only after that can QoS sending token function take effect.

Example

Set the number of QoS sending tokens to 1.

```
[3Com-Ethernet0] qmtoken 1
```

1.21 qos apply policy

Syntax

qos apply policy [**inbound** | **outbound**] *policy-name*

undo qos apply policy [**inbound** | **outbound**]

View

Interface view

Parameter

inbound: Inbound direction.

outbound: Outbound direction.

policy-name: Policy name.

Description

Using the **qos apply policy** command, you can attach an associated QoS policy to an interface. Using the **undo qos apply policy** command, you can delete associated QoS policy from an interface.

If the sum of the bandwidths specified for the assured and expedited forwarding classes in a QoS policy exceeds the available bandwidth on the interface, the policy cannot be applied on the interface. When the available bandwidth on the interface is modified, the policy will be deleted if the sum of the bandwidths specified for the assured and expedited forwarding classes exceeds the available bandwidth on the interface. **af**, **ef**, **wfq** and **gts** cannot be configured for inbound policies.

The application rule of QoS policy in interface view is as follows.

- On a common physical interface or the VT invoked by MP, you can apply the policy configured with various features, including remark, car, gts, af, ef, wfq and wred.
- The policy configured with gts, ef, af and wfq cannot be configured on an inbound interface as an inbound policy.
- Sub-interface does not support queue (ef, af and wfq) feature but support TS (gts) and TP (car). Therefore, the policy configured with TS and TP only can be applied to a sub-interface.

Example

Apply the policy 3COM in the outbound direction of Ethernet0.

```
[3Com-Ethernet0] qos apply policy outbound 3COM
```

1.22 qos class

Syntax

qos class [**logic-and** | **logic-or**] *class-name*

undo qos class [**logic-and** | **logic-or**] *class-name*

View

System view.

Parameter

logic-and: Specify the relation between the rules in the class as logic AND. That is, the packet that matches all the rules belongs to this class.

logic-or: Specify the relation between the rules in the class as logic OR. That is, the packet that matches any one of the rules belongs to this class.

class-name: Class name.

Description

Using the **qos class** command, you can define a QoS policy and enter class view. Using the **undo qos class** command, you can delete a class.

By default, the relation is **logic-and**.

class-name cannot be set to default-class.

For the related commands, see **qos policy**, **qos apply policy**.

Example

Define a class named class1.

```
[3Com] qos class class1
[3Com-qosclass-class1]
```

1.23 qos max-bandwidth

Syntax

qos max-bandwidth *kilobits*

undo qos max-bandwidth

View

Interface view

Parameter

kilobits: Maximum bandwidth in kbit/s of the interface. It ranges from 1 to 1000000.

Description

Using **qos max-bandwidth** command, you can set the maximum bandwidth of an interface. Using **undo qos max-bandwidth** command, you can remove the setting of the maximum bandwidth.

By default, the maximum bandwidth is not configured for all interfaces.

The bandwidth set by this command is only a logic value, not the actual bandwidth of an interface. It is suggested that this value not be configured on a common physical interface, as it is only used for CBQ bandwidth calculation. The actual bandwidths of some interfaces, such as virtual template interface, physical interface configured with Line-Rate and DTE interface used for bandwidth negotiation, are unavailable. Therefore this command is usually configured on these interface.

Note: When the actual available bandwidth (the maximum bandwidth multiplied by the percentage of reserved bandwidth) of an interface is smaller than the sum of the bandwidths (including class-related bandwidths of CBQ and the sum of RTP bandwidths) configured by the user, the configuration of enabling CBQ or RTP on the interface will be automatically canceled due to lack of bandwidth. If the configured bandwidth only fits into one of above requirements, the CBQ configuration will be reserved preferentially.

For the related command, see **qos reserved-bandwidth**.

Example

Set the bandwidth of Virtual-Template 1 to 128kbit/s.

```
[3Com-Virtual-Template1] qos max-bandwidth 128
```

1.24 qos policy

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

View

System view.

Parameter

policy-name: Policy name.

Description

Using **qos policy** command, you can define a policy and enter map view. Using **undo qos policy** command, you can delete a policy.

The policy cannot be deleted if it is applied on an interface. It is necessary to remove application of the policy on the current interface before deleting it via the **undo qos policy** command.

For the related commands, see **qos class**, **qos apply policy**.

Example

Define a policy named 3COM.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com]
```

1.25 qos reserved-bandwidth

Syntax

qos reserved-bandwidth pct *percent*

undo qos reserved-bandwidth

View

Interface view

Parameter

pct *percent*: Percentage of reserved bandwidth in available bandwidth, ranging from 1 to 100. By default, it is 75.

Description

Using **qos reserved-bandwidth** command, you can set the percentage of the maximum reserved bandwidth in available bandwidth. Using **undo qos reserved-bandwidth** command, you can recover the default configuration.

While allocating bandwidth for a QoS queue, considering that part of the bandwidth is used for controlling protocol packets and L2 header, it is suggested that the bandwidth be not larger than 75% of total bandwidth.

For the related command, see **qos max-bandwidth**.

Example

Set the percentage of the maximum reserved bandwidth allocated to the RTP queue application to 70% of the available bandwidth.

```
[3Com-Serial0] qos reserved-bandwidth pct 70
```

1.26 qos-class

Syntax

qos-class *class-name*

undo qos-class *class-name*

View

Class view

Parameter

class-name: Name of class. It is a predefined class name and can be set to "default-class".

Description

Using **qos-class** command, you can configure a class in QoS policy. Using **undo qos-class** command, you can delete the specified class.

For the related command, see **qos policy**.

Example

Configure the class "database" in the QoS policy "3Com", and enter map view.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database]
```

1.27 queue-length

Syntax

queue-length *queue-length*

undo queue-length *queue-length*

View

Policy-class view

Parameter

queue-length: Maximum threshold value of the queue in the range of 1 to 1024. The default drop mode is tail drop.

Description

Using **queue-length** command, you can configure maximum queue length. Using **undo queue-length** command, you can delete configuration.

This command can be used only after the **af** or **wfq** command is configured.

If you run the **undo af** command after configuring the **queue-length** command, the latter will be deleted at the same time.

After configuring **queue-length**, if you enable random drop with the **wred** command, the former will be canceled.

By default, tail drop is configured.

For the related command, see **qos policy**, **qos-class**.

Example

Configure tail drop and the maximum queue length as 16.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database] af bandwidth 200
[3Com-qospolicy-c-3Com database] queue-length 16
```

1.28 remark ip-dscp

Syntax

remark ip-dscp *value*

undo remark ip-dscp *value*

View

Policy-class view

Parameter

value: DSCP value in the range of 0 to 63, which can be any of the following keys: **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5** or **cs7**.

Description

Using **remark ip-dscp** command, you can configure the DSCP value for a class to identify the matched packets. Using **undo remark ip-dscp** command, you can delete the DSCP value.

For the related command, see **qos policy**, **qos-class**.

Example

Configure DSCP value as 6.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database] remark ip-dscp 6
```

1.29 remark ip-precedence

Syntax

remark ip-precedence *value*

undo remark ip-precedence *value*

View

Policy-class view

Parameter

ip-precedence *value*: IP precedence value in the range of 0 to 7.

Description

Using **remark ip-precedence** command, you can configure precedence value to identify matched packets. Using undo set ip precedence command, you can delete precedence value set for a class to identify matched packets.

For the related command, see **qos policy**, **qos-class**.

Example

Configure precedence value to 6 to identify packets.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database] remark ip-precedence 6
```

1.30 wfq

Syntax

wfq [**queue-number** *total-queue-number*]

undo wfq

View

Policy-class view

Parameter

total-queue-number: Number of fair queue, which can be 16, 32, 64, 128, 256, 512, 1024, 2048 and 4096 and the default value is 64.

Description

Using **wfq** command, you can configure the default-class to use WFQ. Using **undo wfq** command, you can delete the configuration.

This command is available for default-class only. In addition, it can be used in cooperation with **queue-length** or **wred.**

For the related command, see **qos policy**, **qos-class**.

Example

Configure WFQ for default-class and the queue number is 16.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class default-class
[3Com-qospolicy-c-3Com default-class] wfq queue-number 16
```

1.31 wred

Syntax

wred [**ip-dscp** | **ip-precedence**]

undo wred [**ip-dscp** | **ip-precedence**]

View

Policy-class view

Parameter

ip-dscp: Indicate that DSCP value is used when calculating drop proportion for a packet.

ip-precedence: Indicate that IP precedence value is used when calculating drop proportion for a packet. By default, **ip-precedence** is configured.

Description

Using **wred** command, you can configure drop mode as WRED. Using **undo wred** command, you can delete the configuration.

To use this command, the **af** command must have been configured. For default-class, the **af** or **wfq** command must be configured before using the command.The **wred** and **queue-length** commands cannot be configured at a time. When canceling this configuration, the WRED-related configuration will be deleted. When a policy configured with **wred** is applied on an interface, the previous WRED configuration on interface will become ineffective.

For default-class, only **ip-precedence** can be configured.By default, the parameter of **wred** is **ip-precedence**.

For the related command, see **qos policy**, **qos-class**.

Example

Configure WRED for a behavior named database and drop proportion is calculated by IP precedence.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database] wred
```

1.32 wred ip-dscp

Syntax

wred ip-dscp *value* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred ip-dscp *dscp-value*

View

Policy-class view

Parameter

value: DSCP value in the range of 0 to 63, which can be any of the following keys: **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5** or **cs7**.

low-limit: Lower threshold value in the range of 1 to 1024. It is 10 by default.

high-limit: Upper threshold value in the range of 1 to 1024. It is 30 by default.

discard-prob: Denominator of drop proportion in the range of 1 to 255. It is 10 by default.

Description

Using **wred ip-dscp** command, you can set DSCP lower-limit, upper-limit and drop proportion denominator of WRED. Using **undo wred ip-dscp** command, you can delete the configuration.

This command can be used only after the **wred** command is used to enable the WRED drop mode based on DSCP.

The configuration of **wred ip-dscp** will be deleted if the configuration of **wred** is deleted.

The configuration of drop parameters will be deleted if **af** is deleted.

For the related command, see **qos policy**, **qos-class**.

Example

Set the queue lower-limit to 20, upper-limit to 40 and discard probability to 15 for the packet whose DSCP is 3.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database] wred ip-dscp
[3Com-qospolicy-c-3Com database] wred ip-dscp 3 low-limit 20 high-limit 40
discard-probability 15
```

1.33 wred ip-precedence

Syntax

wred ip-precedence *value* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred ip-precedence *value*

View

Policy-class view

Parameter

value: Precedence of IP packets in the range of 0 to 7.

low-limit: Lower threshold value in the range of 1 to 1024. It is 10 by default.

high-limit: Upper threshold value in the range of 1 to 1024. It is 30 by default.

discard-prob: Denominator of drop proportion in the range of 1 to 255. It is 10 by default.

Description

Using **wred ip-precedence** command, you can set precedence lower-limit, upper-limit and drop proportion denominator of WRED. Using **undo wred ip-precedence** command, you can remove the configuration.

This command can be used only after the **wred** command has been used to enable WRED drop mode based on DSCP. The configuration of **wred** will be deleted if the configuration of **qos wred** is deleted.

The configuration of drop parameters will be deleted if **af** is deleted.

For the related command, see **qos policy**, **qos-class**.

Example

Set lower-limit to 20, upper-limit to 40 and discard probability to 15 for the packet with the precedence 3.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database] wred
[3Com-qospolicy-c-3Com database] wred ip-precedence 3 low-limit 20 high-limit
40 discard-probability 15
```

1.34 wred weighting-constant

Syntax

wred weighting-constant *exponent*

undo wred weighting-constant

View

Policy-class view

Parameter

exponent: Exponential in the range of 1 to 16. It is 6 by default.

Description

Using **wred weighting-constant** command, you can set exponential for the calculation of average queue length by WRED. Using **undo wred weighting-constant** command, you can remove the configuration.

Before using this command, you must have configured the **af** command and have used the **wred** command to enable the WRED discarding mode.

When removing the **wred** configuration, the configuration of **wred weighting-constant** is deleted at a time.

For the related command, see **qos policy**, **qos-class**.

Example

Configure exponential for calculating average queue to 6.

```
[3Com] qos policy 3Com
[3Com-qospolicy-3Com] qos-class database
[3Com-qospolicy-c-3Com database] af bandwidth 200
[3Com-qospolicy-c-3Com database] wred ip-precedence
[3Com-qospolicy-c-3Com database] wred weighting-constant 6
```

Chapter 2 TACACS+ Configuration Commands

2.1 debugging hwtacacs

Syntax

debugging hwtacacs { authentication | authorization | accounting } [packet] [user *user-name*][interface *interface-name*]

undo debugging hwtacacs { authentication | authorization | accounting } [packet] [user *user-name*][interface *interface-name* | { *interface-type interface-number* }]

View

All views

Parameter

authentication: Enable AAA authentication debugging and display the authentication debugging information.

authorization: Enable AAA authorization debugging and display the authorization debugging information.

accounting: Enable AAA accounting debugging and display the AAA accounting debugging information.

packet: Enable AAA packets debugging and print the details of AAA packets.

user *user-name*: User name, which is a printable string of 1 to 32 characters except for the space.

interface *interface-name*: The name of the port where a user logs in, which is represented by interface and interface number, i.e. interface Serial0.

interface-type interface-number: Interface name and number.

Description

Using **debugging hwtacacs** command, you can enable debugging on the AAA implementation using TACACS+. Using **undo debugging hwtacacs** command, you can disable debugging on the AAA implementation using TACACS+.

By default, AAA debugging is disabled.

Using **debugging hwtacacs authentication** command, you can display the authentication information and the authorization state of the current users. If the command is not configured with any argument, the information of all the users will be displayed. If the argument **user** has been configured, only the authentication information of the specified user will be displayed. If only the argument **interface** has been defined for the command, only the user authentication information on the interface will be displayed. If only packet has been defined for the command, only the TACACS+ packets received and transmitted on the router will be displayed.

Example

Enable AAA authentication debugging.

```
[Router] debugging hwtacacs authentication
```

2.2 display hwtacacs accounting

Syntax

display hwtacacs accounting [verbose]

View

All views

Parameter

verbose: Display the detailed accounting information of AAA users. If this argument has been configured, the information sorted by user type will be displayed in addition to other information.

Description

Using **display hwtacacs accounting** command, you can display all accounting information.

The **display hwtacacs accounting** command can be used to display all the events on which accounting can be made. Executing this command will display all the active accounting records, user names, names of the interfaces used by the users, the ID, and type and duration (including the abbreviation of the time zone) of each accounting session, as well as the service type. In addition, the length of the current accounting queue will also be displayed.

For related command, see reset accounting statistics.

Example

Display the accounting information of AAA users.

```
[3Com]display hwtacacs accounting
   Hwtacacs Accounting Statistics
   Accounting Packet Wait-Queue Length: 0
   Username don
   Accounting time=00:01:19
   Accounting type=Login,Service=SHELL
------------------------------------------------------------
   Username don
   Accounting time=00:00:12
   Accounting type=Login,Service=SHELL
------------------------------------------------------------
```

Display the accounting verbose of AAA users.

```
[3Com]display hwtacacs accounting verbose
   Hwtacacs Accounting Statistics
   Accounting Packet Wait-Queue Length: 0
   Accounting type:Login
   Starts=2 Stops=0 realtimes=0 Active=0 Drops=0
   Accounting type:Network
   Starts=0 Stops=0 realtimes=0 Active=0 Drops=0
   Accounting type:Outbound
   Starts=0 Stops=0 realtimes=0 Active=0 Drops=0
   Accounting type:Command
   Starts=0 Stops=15 realtimes=0 Active=0 Drops=0
   Accounting type:System
   Starts=0 Stops=0 realtimes=0 Active=0 Drops=0

   Username don
   Accounting time=00:01:25
   Accounting type=Login,Service=SHELL
------------------------------------------------------------
   Username don
   Accounting time=00:00:18
   Accounting type=Login,Service=SHELL
------------------------------------------------------------
```

Table 2-1 Field description of the display hwtacacs accounting command

Item	Description
interface	Interface used by a user, which can be any type of interfaces listed as follows: Physical interfaces: Synchronous serial interface, asynchronous serial interface, Ethernet interface, AUX interface, console interface, Asynchronous Modem (AM) interface Logical interface: dialer interface, loopback interface, tunnel interface, virtual-template interface
Username	User name
Accounting type	Accounting session type, which can be Login, Network, Outbound, Command or System
Accounting time	The duration of this type of session in hh:mm:ss.
Service	It can be PPP, shell, connection or system.
Protocol	The protocol of the service subset, which can be TCP, IP, IPX, Telnet, Rlogin, pad, VPDN, multilink, or unknown.
Address	IP address of users accessing the router
Login	Display the accounting information of Login sessions (the user shell program)
PPP	Display the accounting information of all the network service requests.
Outbound	Provide all the outbound connection information (Telnet, rlogin, PAD) generated by the NAS.
Command	Display the statistics of all the commands at the specified level.
System	Display the statistics of the system events.
Starts	The times that the accounting of each type has been started
Stops	The times that the accounting of each type has been stopped.
Realtimes	The times that the accounting of each type has been updated.
Active	The number of active accounting of each type.
Drops	The number of the dropped accounting packets for each accounting type when the sending queues have been full.

2.3 display hwtacacs server

Syntax

display hwtacacs server [verbose]

View

All views

Parameter

verbose: Display information of the authentication and authorization and accounting queues of AAA users as well as the TACACS+ server information.

Description

Using the **display hwtacacs server** command, you can display the verbose information between the local device and the TACACS+ server.

Using the **display hwtacacs server** command, you can display the times that an TACACS+ server enables and disables the TCP connection, the number of

AUTHENTICATION TERMINATE packets sent by the router, the received and transmitted packets, and the number of connection failures.

Using the **display hwtacacs server verbose** command, you can display the size of the accounting, authorization and accounting queues of AAA users, whether the queue has been fully occupied, and the message displayed when the queues are full.

For a related command, see **reset hwtacacs server statistics**.

Example

Display the information interacted between the current host and the TACACS+ server.

```
[Router]display hwtacacs server  verbose
                     Queue length   Current Queue length
Authentication          250                  1
Authorization           250                  1
Accounting              250                  1

    0       0      0      0
   Aborts       Errors     Timeout   Connect_fails
------------------------------------------------------------------------
    0       0      0      0
   Aborts       Errors     Timeout   Connect_fails
------------------------------------------------------------------------
    0       0      0      0
   Aborts       Errors     Timeout   Connect_fails
------------------------------------------------------------------------
    0       0      0      0
   Aborts       Errors     Timeout   Connect_fails
------------------------------------------------------------------------
[Router]display hwtacacs server
                     Queue length   Current Queue length
Authentication          250                  1
Authorization           250                  1
Accounting              250                  1
```

2.4 domain

Syntax

domain

undo domain

View

Hwtacacs view

Parameter

None

Description

Using **domain** command, you can configure a specified TACACS+ server to permit a user to directly specify the domain name when entering the user name. Using **undo domain** command, you can disallow a specified TACACS+ server to permit the user to directly specify the domain name when entering the user name.

For example:

If the user configures the domain command, the router will only send “username” to the TACACS+ server when username@3com.com is entered.

By default, a user is not allowed to directly specify the domain name.

If **undo domain** has been executed, the whole character string entered by a user will be sent to the TACACS+ server configured in the scheme as the user name. For example, if a user enters username@3com.com, the router will send the whole string as the user name to the TACACS+ server specified in the scheme.

Example

Configure the server group **tactemplate1** to support the operation of directly specifying domain name.

```
[3Com]hwtacacs-server template tactemplate1
[3Com-hwtacacs-tactemplate1]domain
```

2.5 host

Syntax

host ip *ip-address* [port *port-number*] [response-timeout *time*] [shared-key *key-string*] [authen-primary | author-primary | account-primary]

undo host ip *ip-address* [authen-primary | author-primary | account-primary]

View

Hwtacacs view

Parameter

ip *ip-address*: IP address of the TACACS+ server to be added.

name *host-name*: Name of the TACACS+ server to be added, which has been configured by the **IP host** command. It is a string of 1 to 20 printable characters except for the space.

port *port-number*: The service port number on the TACACS+ server, which is in the range of 1 to 65535.

response-timeout *time*: The response timeout time of TACACS+ server, which is in the range of 1 to 1000 seconds and defaults to 5 seconds.

shared-key *key-string*: The encrypted key for the AAA negotiation between the Router and the TACACS+ server. It is a string of printable characters (except for the space) of 1 to 64 characters in length. By default, the key configured using the **shared-key** command is used.

authen-primary: Specify the server configured currently as the primary authentication server.

author-primary: Specify the server configured currently as the primary authorization server.

account-primary: Specify the server configured currently as the primary accounting server.

Description

Using **host** command, you can add a TACACS+ server into a TACACS+ server group by specifying its IP address as well as specifing it as the primary AAA server. Using **undo host** command, you can delete a TACACS+ server from a TACACS+ server group by specifying its IP address or you can disable it as the AAA primary server.

By default, no TACACS+ server is configured.

A server group allows of a maximum of five TACACS+ servers.

You can use the parameters **authen-primary**, **author-primary**, or **account-primary** to specify the current configured TACACS+ server as the specified primary authentication, authorization, or accounting server. If none of the servers in a sever group has been specified as the primary server, the first one will be the primary server.

If a primary server has been specified, and if the current AAA server is a standby server, the switch interval specified by the **timer quiet** command in hwtacacs view will be used to perform the standby/primary switchover operation. Otherwise, no switch will be performed.

Each TACACS+ server group allows only one primary authentication server, one primary authorization server, and one primary accounting server. When you configure a second primary server, there will be prompt information, the previous primary AAA server will be changed into a common server, and the newly configured server will be taken as the primary one.

If the number of servers configured in a template exceeds the allowed upper threshold, the following prompt will be displayed:

```
Warning: Reach the max limited of server in one template.
```

If the *host-name* argument has not been mapped to an IP address using the **ip host** command, the configuration will fail, and the following prompt will be displayed:

```
Warning: no such host.
```

If the specified server to be deleted using the **undo host** command is the specified primary AAA server in the server group, the following prompts will be displayed:

```
Warning: The Server is a authen-primary Server.
Warning: The Server is a author-primary Server.
Warning: The Server is a account-primary Server.
```

If configuring **undo host** with the parameter **authen-primary** or **author-primary** or **account-primary**, you will only disable the primary server property of the server rather than removing the server from the server group.

When you attempt to configure a second primary authentication, authorization, or accounting server, the following prompts will be displayed:

```
Warning: Only permit one authen-primary Server.
Warning: Only permit one author-primary Server.
Warning: Only permit one account-primary Server.
```

For related commands, see hwtacacs-server template and timer quiet.

Example

Configure TACACS+ servers in the TACACS+ server group tactemplate1, and specify the server at 1.1.1.1 as the primary AAA server in tactemplate1.

```
[Router] hwtacacs-server template tactemplate1
[Router-hwtacacs-tactemplate1]host ip 1.1.1.1 authen-primary
[Router-hwtacacs-tactemplate1] host ip 1.1.1.1 author-primary
[Router-hwtacacs-tactemplate1] host ip 1.1.1.1 account-primary
[Router-hwtacacs-tactemplate1] host ip 1.1.1.2
```

2.6 hwtacacs-server template

Syntax

hwtacacs-server template *template-name*

undo hwtacacs-server template *template-name*

View

System view

Parameter

template-name: The string naming a server group, which contains 1 to 20 printable characters except for the space.

Description

Using **hwtacacs-server template** command, you can create a TACACS+ server group by specifying the name. Using **undo hwtacacs-server template** command, you can delete an TACACS+ server group by specifying its name.

By default, no TACACS+ server group has been created.

With this command, a maximum of 11 TACACS+ server groups can be configured, with each containing up to 5 TACACS+ servers.

If the template configured currently exceeds the upper threshold, the following prompt will be displayed:

```
Warning: reach the max limited of aaa template server hwtacacs.
```

For related commands, see **host**, **timer quiet**, and **domain**.

Example

Configure a TACACS+ server group named “hwtemplate1”, which has three TACACS+ member servers.

```
[Router]hwtacacs-server template hwtemplate1
[Router-hwtacacs-hwtemplate1] host ip 1.1.1.1
[Router-hwtacacs-hwtemplate1] host ip 1.1.1.2
[Router-hwtacacs-hwtemplate1] host ip 1.1.1.3
```

2.7 reset hwtacacs accounting statistics

Syntax

reset hwtacacs accounting statistics

View

All views

Parameter

None

Description

Using **reset hwtacacs accounting statistics** command, you can clear all accounting statistics for AAA users.

For a related command, see **display hwtacacs accounting**.

Example

Clear all accounting statistics for the AAA users.

```
[Router] reset hwtacacs accounting statistics
```

2.8 reset hwtacacs server statistics

Syntax

reset hwtacacs server statistics

View

All views

Parameter

None

Description

Using **reset hwtacacs server statistics** command, you can clear all statistics for TACACS+ servers.

For a related command, see **display hwtacacs server**.

Example

Clear all the statistics of TACACS+ servers.

```
[Router] reset hwtacacs server statistics
```

2.9 shared-key

Syntax

shared-key *key-string*

undo shared-key

View

Hwtacacs view

Parameter

key-string: The encrypted key used for the AAA negotiation between the router and a TACACS+ server. It is a string of 1 to 64 printable characters (except for the space) in length and must match the key used by the TACACS+ server.

Description

Using the **shared-key** command, you can set a shared key for the router and a TACACS+ server to carry out AAA negotiation. Using **undo shared-key** command, you can delete the shared key used for the AAA negotiation with the TACACS+ server.

By default, no key is set.

The entered key must match the key used by the TACACS+ server. All the leading spaces in the key string will be ignored, and the keys containing spaces will not be supported.

The key configured using this command will be replaced by the one configured using the command **host**.

For related command, see **host**.

Example

Use “mykey” as the encrypted key for the AAA negotiation with the TACACS+ server.

```
[Router] hwtacacs-server template tactemplate1
[Router-hwtacacs-tactemplate1] shared-key mykey
```

2.10 source-ip

Syntax

source-ip { ip-address | **interface** interface-type interface-number }

undo source-ip

View

Hwtacacs view

Parameter

ip-address: The source IP address of all the TACACS+ packets.

interface-type: Interface type, such as serial.

interface-number: Interface number, including the main interface number and the sub-interface number.

Description

Using the **source-ip** command, you can specify a source IP address for the TACACS+ packets transmitted from the Router. Using **undo source-ip** command, you can disable specifying a source IP address for the TACACS+ packets.

By default, no IP address is specified for transmitting TACACS+ packets

If the same source IP address is specified for all the TACACS+ packets, the TACACS+ server will only need to contact the router using that IP address, instead of registering the IP addresses of all the interfaces that are likely to send TACACS+ packets.

An IP address must be assigned to the specified interface.

Only one source IP address can be configured for a TACACS+ server group, but different source IP addresses can be configured for different groups.

Example

TACACS+ takes the IP address of the interface Loopback 1 as the source IP address of all the TACACS+ packets.

```
[Router] hwtacacs-server template tactemplate1
[Router-hwtacacs-tactemplate1]source-ip interface loopback 1
```

2.11 timer quiet

Syntax

timer quiet *minute*s

undo timer quiet

View

Hwtacacs view

Parameter

minutes: Switchover interval, which must be in the range of 1 to 255 minutes and defaults to 5 minutes.

Description

Using the **timer quiet** command, you can configure a standby/primary server switchover interval in case the current AAA service is provided by a standby server in the specified TACACS+ server group. Using **undo timer quiet** command, you can restore the default standby/primary switchover interval.

You must configure the **hwtacacs-server template** command and enter the hwtacacs view before configuring this command.

This switchover interval can become valid only if you have specified a AAA primary server with the arguments **authen-primary**, **author-primary**, or **account-primary** when configuring the **host** command. Otherwise, no standby/primary server switchover will be performed.

For related commands, see **hwtacacs-server template** and **host**.

Example

Set the standby/primary switchover interval for the TACACS+ server group tactemplate1 to three minutes.

```
[Router]hwtacacs-server template tactemplate1
[Router-hwtacacs-tactemplate1] host ip 1.1.1.1 authen-primary
[Router-hwtacacs-tactemplate1] host ip 1.1.1.2 author-primary
[Router-hwtacacs-tactemplate1] timer quiet 3
```

Chapter 3 SSH Configuration Commands

3.1 debugging rsa

Syntax

debugging rsa

undo debugging rsa

View

All views

Parameter

None

Description

Using the **debugging rsa** command, you can enable RSA debugging and send the details of all the processes and the packet structure of the RSA algorithm to the info-center in the form of debugging information. Using the **undo debugging rsa** command, you can disable debugging.

By default, debugging is disabled.

For related commands, see **rsa local-key-pair create**, and **rsa local-key-pair destroy**.

Example

Enable RSA debugging.

```
[3Com] debugging rsa
```

3.2 debugging ssh server

Syntax

debugging ssh server { **VTY** *index* | **all** }

undo debugging ssh server { **VTY** *index* | **all** }

View

User view

Parameter

VTY *index*: The SSH channel being debugged. Its value is a VTY number and is in the range of 0 to 4 by default.

all: All the SSH channels.

Description

Using the **debugging ssh server** command, you can send the information such as the negotiation procedure provisioned in SSH1.5 to the info-center in the form of debugging information. Using the **undo debugging ssh server** command, you can disable debugging.

By default, debugging is disabled.

For related commands, see **ssh server authentication-retries**, **ssh server rekey-interval**, and **ssh server timeout**.

Example

Print the debugging information when running SSH.

```
[3Com] debugging ssh server vty 4
  SSH: The packet received on VTY 4
  SSH: SSH_CMSG_STDIN_DATA message received on VTY 4
  SSH: 3DES encrypt on VTY 4
  SSH: The ssh packet sent on VTY 4
  SSH: SSH_SMSG_STDOUT_DATA message sent on VTY 4
  SSH: 3DES encrypt on VTY 4
  SSH: The ssh packet sent on VTY 4
  SSH: SSH_SMSG_STDOUT_DATA message sent on VTY 4
  SSH: 3DES encrypt on VTY 4
  SSH: The ssh packet sent on VTY 4
  SSH: SSH_SMSG_STDOUT_DATA message sent on VTY 4
```

3.3 display rsa local-key-pair public

Syntax

display rsa local-key-pair public

View

All views

Parameter

None

Description

Using the **display rsa local-key-pair public** command, you can display the public key portion of the server-end host key-pair and server key-pair. If no key has ever been created, the system will inform you that it has not found any keys by displaying “RSA keys not found” for example.

For related command, see **rsa local-key-pair create**.

Example

```
[3Com] display rsa local-key-pair public
=====================================================
Time of Key pair created: 14:20:8  2000/12/13
Key name: 3Com_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    D5797459 00089D88 A3CB8FE2 58B81738 56E915CF
    56CF4CAD 68092873 7692C033 98B2C7C5 DECA9BFB
    2238AFBC 9FC6D888 7265682C DA989C40 46A14143
    452F97F7
  0203
    010001

=====================================================
Time of Key pair created: 14:20:13  2000/12/13
Key name: 3Com_Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    B4CE981E 5570003C DB2E98B7 AABF0E4D 7FC12C05
    97BFA718 6AD12204 A8AB1C9C A41B4DC2 E0389F63
```

```
  CF8EBE33 42C71357 FC241E4F DEB64C09 DA06995C
  99859934 25F6800A AB8859BE 0F83FC63 15A3115C
  BD3A15E7 D52DCE19 324DBBF9 58DB936B
0203
  010001
```

3.4 display rsa peer-public-key

Syntax

display rsa peer-public-key [**brief** | **name** *keyname*]

View

All views

Parameter

brief: Displays the brief information of all the remote public keys.

keyname: Name of the key to be displayed, which is a string of 1 to 64 consecutive characters.

Description

Using the **display rsa peer-public-key** command, you can display information of a specified RSA public key. If no key has been specified, the information of all the RSA public keys will be displayed.

For related command, see **rsa local-key-pair create**.

Example

```
[3Com] display rsa peer-public-key brief
Address       Bits   Name
--------------------------
              1024   key2
              1024   key_smith
[3Com]display rsa peer-public-key name key2

=====================================
   Key name: key2
   Key address:
=====================================
```

```
Key Code:
308186
  028180
    E75E3D7C 11923D33 143FB829 470EA018 889147F6 6F27A98A D6C54A36 C7DB17E1
    647DC2BE F1C54116 641CD690 E5F7B492 A059BD6A B86A7D18 1040765C 978AF7C9
    12807EAE 819B4A65 787CDE9C 940F74C8 BC4EFD81 6CC3EBDA 51E75D1B D073AA69
    1F646A81 035496AC 6F98A730 D8C44931 598682EF EA40DF88 5DD98D45 2670231D
  0201
    25
```

3.5 display ssh server

Syntax

display ssh server { **status | session** }

View

All views

Parameter

status: Display the status information of the SSH server.

session: Display the session information of the SSH server.

Description

Using the **display ssh server** command, you can display the SSH state or session information.

For related commands, see **ssh server authentication-retries**, **ssh server rekey-interval**, and **ssh server timeout**.

Example

Display SSH state and configuration parameters.

```
[3Com] display ssh server status
SSH version : 1.5
SSH connection timeout : 60 seconds
SSH server key generating interval : 1 hours
SSH Authentication retries : 3 times
```

Display SSH sessions.

```
[3Com] display ssh server session
Connection    Version Encryption   State           Username
```

```
VTY0          1.5      DES          Session started  3Com
VTY3          1.5      DES          Session started  router
```

3.6 display ssh user-information

Syntax

display ssh user-information [*username*]

View

All views

Parameter

username: A valid SSH user name defined by AAA.

Description

Using the **display ssh user-information** command, you can display information of the current SSH users, including usernames, key names associated with the users, and the authentication types of the user. If the parameter *username* has been specified, only information of the specified user will be displayed.

For related commands, see **ssh user username assign rsa-key**, **ssh user username authentication-type**.

Example

Display user information.

```
[Router] display ssh user-information
Username      authentication-type     user-public-key-name
1000              rsa                 file3
4000              all                 hq_rsa
smith_rsa         rsa                 hq_rsa
smith_all         all                 hq_all
```

3.7 hex

Syntax

hex *hex-data*

View

Public key edit view

Parameter

hex-data: Public key data, which is a hexadecimal character string coded in the public key format.

Description

Using the **hex** command, you can input the public key data.

The public key that you input must be the one randomly generated by the SSH client program. You are allowed to input spaces in the character string to separate the characters, generally according to the format that the public key data are arranged, for the purpose of convenient input and later check.

After inputting all the public key data, use the **public-key-code end** command to end the editing of the public key. Before saving the key, the system will verify the validity of the key. If there is any illegal character in the character string, the system will prompt that it will discard all the public key data configured by the user due to the presence of illegal characters and will return to the public key view from the current view. In this case, you can access the public key edit view again using the **public-key-code begin** command and input new public key data using the **hex** command.

For related commands, see **public-key-code begin**, and **public-key-code end**.

Example

Input invalid character string when configuring a public key.

```
[3Com] rsa peer-public-key mykey
[3Com-rsa-public] public-key-code begin
[3Com-rsa-key-code] hex abcdefg
% Invalid input.
[3Com-rsa-key-code] public-key-code end
% Invalid key string, the length is zero.
```

Input a valid character string when configuring a public key.

```
[3Com] rsa peer-public-key mykey
[3Com-rsa-public-key] public-key-code begin
[3Com-rsa-key-code] hex 308186
[3Com-rsa-key-code] hex 028180
[3Com-rsa-key-code] hex E75E3D7C 11923D33 143FB829 470EA018 889147F6 6 F27A98A
D6C54A36
```

```
[3Com-rsa-key-code] hex C7DB17E1 647DC2BE F1C54116 641CD690 E5F7B492 A 059BD6A
B86A7D18
[3Com-rsa-key-code] hex 1040765C 978AF7C9 12807EAE 819B4A65 787CDE9C 9 40F74C8
BC4EFD81
[3Com-rsa-key-code] hex 6CC3EBDA 51E75D1B D073AA69 1F646A81 035496AC 6 F98A730
D8C44931
[3Com-rsa-key-code] hex 598682EF EA40DF88 5DD98D45 2670231D
[3Com-rsa-key-code] hex 0201
[3Com-rsa-key-code] hex 25
[3Com-rsa-key-code] public-key-code end
[3Com]
```

3.8 kill ssh

Syntax

kill ssh { **all** | **userID** *userid* }

View

System view

Parameter

all: Closes all the current SSH processes by force.

userID *userid*: Closes the SSH process specified by the task ID by force.

Description

Using the **kill ssh** command, you can close an SSH process by force.

A system administrator can disconnect the connections of all the SSH login users by force by executing the **kill** command on the console interface, or close by force the SSH process of a specified SSH login user found by executing the **display local-user online** command..

For related command, see **display local-user**.

Example

View the SSH processes of the specified tasks on the router.

```
[3Com]display local-user online
TaskID InterfaceName  UserName  HostName(s)  Location  IdleTime
16    Console                                  01:05:29
36    Ethernet0       smith    169.254.1.1 169.254.231.179 00:00:11
```

Close the SSH process of task 36 on the router.

```
[3Com] kill ssh userid 36
```

3.9 protocol inbound

Syntax

protocol inbound { **ssh** | **telnet** } *numbers* [**acl** *acl-number*]

View

System view

Parameter

ssh: Supports SSH.

telnet: Supports Telnet..

numbers: Specifies the maximum number of connections that the protocol is allowed to set up. It is in the range of 0 to 5, with 0 indicating that the protocol is not supported. By default, the allowed maximum number of Telnet connections is 5 and no SSH connection is allowed.

acl *acl-number*: Specifies the number of a basic ACL for an IP address. It is in the range of 0 to 99, with 0 indicating that no ACL is used.

Description

Using the **protocol inbound** command, you can specify the protocol and the maximum number of the protocol specific connections that the system supports. .

The maximum number of Telnet connections defaults to 5 and the maximum number of SSH connections defaults to 0.

Given SSH has been enabled but the RSA key has not been configured on the local device, the SSH user will still be unable to pass the login authentication. The configuration result will take effect the next time when the user logs in the system.

Example

Set the system to support three SSH connections and not to adopt ACL.

```
[3Com] protocol inbound ssh 3
```

3.10 public-key-code begin

Syntax

public-key-code begin

View

Public key view

Parameter

None

Description

Using the **public-key-code begin** command, you can access the public key edit view to input the public key data generated by the client program..

Before using this command, you must specify a key name using the command **rsa peer-public-key** and access the public key edit view. Then, you can input the **public-key-code begin** command and use the **hex** command to input the key data. You can input the key data by using the **hex** command for multiple times.

For related commands, see **rsa peer-public-key**, **public-key-code end**, and **hex**.

Example

Access the public key edit view and input the key data.

```
[3Com] rsa peer-public-key 3Com003
[3Com-rsa-public-key] public-key-code begin
[3Com-rsa-key-code] hex 308186
[3Com-rsa-key-code] hex 028180
[3Com-rsa-key-code]hex E75E3D7C 11923D33 143FB829 470EA018 889147F6 6 F27A98A
D6C54A36
[3Com-rsa-key-code]hex C7DB17E1 647DC2BE F1C54116 641CD690 E5F7B492 A 059BD6A
B86A7D18
[3Com-rsa-key-code]hex 1040765C 978AF7C9 12807EAE 819B4A65 787CDE9C 9 40F74C8
BC4EFD81
[3Com-rsa-key-code]hex 6CC3EBDA 51E75D1B D073AA69 1F646A81 035496AC 6 F98A730
D8C44931
[3Com-rsa-key-code] hex 598682EF EA40DF88 5DD98D45 2670231D
[3Com-rsa-key-code] hex 0201
[3Com-rsa-key-code] hex 25
[3Com-rsa-key-code] public-key-code end
```

3.11 public-key-code end

Syntax

public-key-code end

View

Public key view

Parameter

None

Description

Using the **public-key-code end** command, you can end the public key editing and save the configured public key. Besides, you can also use this command to return from the public key view to the system view.

After ending the public key editing by executing this command, the system will verify the validity of the key before saving the key. If there is any invalid character in the character string, the system will prompt that it will discard all the public key data configured by the user due to the presence of invalid characters and will return to the public key view from the current view . In this case, you can access the public key edit view again using the **public-key-code begin** command and input new public key data using the **hex** command. If you do not want to input the key data again, you can exit to the system view by executing the **public-key-code end** command.

If the system makes sure that the configured key is valid, it will save the public key into the link table of public keys and exit the current view to the system view.

In public key edit view, you are unable to exit to the system view by executing the command **quit** or **return**.

For related commands, see **rsa peer-public-key**, **public-key-code begin**, and **hex**.

Example

Input an invalid character string when configuring a public key.

```
[3Com] rsa peer-public-key mykey
[3Com-rsa-public-key] public-key-code begin
[3Com-rsa-key-code] public-key-code end
% Invalid key string, the length is zero.
```

Input a valid character string when configuring a public key.

```
[3Com] rsa peer-public-key mykey
```

```
[3Com-rsa-public-key] public-key-code begin
[3Com-rsa-key-code] hex 308186
[3Com-rsa-key-code] hex 028180
[3Com-rsa-key-code]hex E75E3D7C 11923D33 143FB829 470EA018 889147F6 6 F27A98A
D6C54A36
[3Com-rsa-key-code]hex C7DB17E1 647DC2BE F1C54116 641CD690 E5F7B492 A 059BD6A
B86A7D18
[3Com-rsa-key-code]hex 1040765C 978AF7C9 12807EAE 819B4A65 787CDE9C 9 40F74C8
BC4EFD81
[3Com-rsa-key-code]hex 6CC3EBDA 51E75D1B D073AA69 1F646A81 035496AC 6 F98A730
D8C44931
[3Com-rsa-key-code] hex 598682EF EA40DF88 5DD98D45 2670231D
[3Com-rsa-key-code] hex 0201
[3Com-rsa-key-code] hex 25
[3Com-rsa-key-code] public-key-code end
[3Com]
```

3.12 rsa local-key-pair create

Syntax

rsa local-key-pair create

View

System view

Parameter

None

Description

Using the **rsa local-key-pair create** command, you can generate RSA host key-pair and server key-pair.

If there has been RSA key, the system will ask if you want to replace the existing key. The generated key-pairs are respectively represented by “router name + server” and “router name + host”. This command will not be saved in the configuration file.

After this command is input, the system will prompt you to enter the bits of the host key. A server key-pair and a host key-pair have the difference of at least 128 bits in size.. Both of them have the same minimum and maximum sizes, i.e., 512 bits and 2048 bits. If there has been a key, the user is required to confirm whether to change the key.

An essential operation underlying a successful SSH login is generating local RSA key-pairs by configuring **rsa local-key-pair create**. It is only necessary for you to execute this command once and you do not have to execute it again after rebooting the router..

For related command, see **rsa local-key-pair destroy**.

Example

Generate the host key pair and server key pair.

```
[3Com] rsa local-key-pair create
The key name will be: 3Com_Host
% RSA keys defined for 3Com_Host already exist.
Confirm to replace them? [yes/no]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
      It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
.................++++++++++++
.............++++++++++++
..............++++++++
.................++++++++
```

The system will display the RSA key generating process information on the screen, where, “.” indicates that the system has generated a random number and is testing whether it is a prime number and “+” means that the system is testing to see whether the prime number meets the requirement.

3.13 rsa local-key-pair destroy

Syntax

rsa local-key-pair destroy

View

System view

Parameter

None

Description

Using the **rsa local-key-pair destroy** command, you can destroy all the server-end RSA keys (including host key-pairs and server key-pairs).

After inputting this command, you are required to confirm whether to destroy all the server-end RSA keys. In addition, this command will not be saved in the configuration file.

For related command, see **rsa local-key-pair create**.

Example

Destroy all the server-end keys.

```
[3Com] rsa local-key-pair destroy
% The name for the keys which will be destroyed is 3Com_Host .
% Confirm to destroy these keys? [yes/no]:y
```

3.14 rsa peer-public-key

Syntax

rsa peer-public-key *key-name*

undo rsa peer-public-key *key-name*

View

System view

Parameter

key-name: Name of the key to be configured/destroyed, which is a character string of 1 to 64 bytes.

Description

Using the **rsa peer-public-key** command, you can access the public key view to configure the public key of the client end. Using the **undo rsa peer-public-key** command, you can delete the specified public key.

You can access the public key view using this command and configure the key of the client end by using the command along with the commands **public-key-code begin** and **public-key-code end**. The public key of the client end is a random key generated by an SSH1.5-enabled client program.

When executing the **undo rsa peer-public-key** command to delete a specified public key, the system will prompt the following information in case the specified key does not exist.

```
% Public key not found.
```

For related commands, see **public-key-code begin**, and **public-key-code end**.

Example

Access the public key view.

```
[3Com] rsa peer-public-key 3Com002
[3Com-rsa-public-key]
```

3.15 ssh server authentication-retries

Syntax

ssh server authentication-retries *times*

undo ssh server authentication-retries

View

System view

Parameter

times: The number of authentication retries, which is in the range of 1 to 5 and defaults to 3.

Description

Using the **ssh server authentication-retries** command, you can set the number of SSH connection authentication retries that are allowed. Using the **undo ssh server authentication-retries** command, you can restore the default maximum number of SSH connection authentication retries that are allowed..

This command is to prevent the illegal activities such as malicious decipherment by limiting the number of SSH connection authentication retries. The configuration will take effect the next time when the use logs in the router.

For related command, see **display ssh server**.

Example

Set the allowed number of login authentication retries to 4.

```
[3Com] ssh server authentication-retries 4
```

3.16 ssh server rekey-interval

Syntax

ssh server rekey-interval *hours*

undo ssh server rekey-interval

View

System view

Parameter

hours: Updating interval which is in the range of 1 to 24 hours.

Description

Using the **ssh server rekey-interval** command, you can set the interval for updating the SSH server key. Using the **undo ssh server rekey-interval** command, you can disable updating the SSH server key..

By default, no updating operation is performed on the key.

For related commands, see **display ssh server**.

Example

Update the server key every three hours.

```
[3Com] ssh server rekey-interval 3
[3Com]
```

3.17 ssh server timeout

Syntax

ssh server timeout *seconds*

undo ssh server timeout

View

System view

Parameter

seconds: Login timeout time, which is in the range of 1 to 120 seconds and defaults to 60 seconds.

Description

Using the **ssh server timeout** command, you can set the login authentication timeout time at the SSH server end. Using the **undo ssh server timeout** command, you can restore the default login authentication timeout time at the server end.

The configuration will take effect the next time when the use logs in the router.

For related command, see **display ssh server**.

Example

Set the login timeout time to 80 seconds.

```
[3Com] ssh server timeout 80
```

3.18 ssh user username assign rsa-key

Syntax

ssh user *username* **assign rsa-key** *keyname*

undo ssh user *username* **assign rsa-key**

View

System view

Parameter

username: A valid SSH username defined by the AAA module, which is a string of 0 to 32 consecutive characters in length with 0 excluded and 32 included.

keyname: Name of the client-side public key, which is a string of 0 to 64 consecutive characters in length with 0 excluded and 64 included.

Description

Using the **ssh user username assign rsa-key** command, you can assign an existing public key to a specified SSH user. Using the **undo ssh user username assign rsa-key** command, you can remove the association between the user and the assigned public key.

The public key that you assign to a user by using this command will replace the one that you have assigned last time.

The AAA module is responsible for the creation and deletion of local usernames in the system. Whenever creating an SSH user, The AAA module will inform SSH whenever it creates an SSH user, and SSH will add the username into the maintained user database. Likewise, the AAA module will inform SSH whenever it deletes a user, and SSH will look up the username database for a match and will delete the matched username, if there is any.

The newly configured public key will take effect the next time when the user logs in the router.

For related command, see display ssh user-information.

Example

Assign the public key *key1* to the user smith.

```
[3Com] ssh user smith assign rsa-key key1
```

3.19 ssh user authentication-type

Syntax

ssh user *username* **authentication-type** { **password** | **RSA** | **all** }

undo ssh user *username* **authentication-type** { **password** | **RSA** | **all** }

View

System view

Parameter

username: The specified username.

password: Specifies the password mode as the authentication mode for the user by force.

RSA: Specifies the RSA mode as the authentication mode for the user by force.

all: The authentication mode of the user can be either password or RSA.

Description

Using the **ssh user username authentication-type** command, you can set an authentication mode for a specified user. Using the **undo ssh user username**

authentication-type command, you can disable the login authentication mode for the user, in which case the user will be unable to log into the system.

By default, no login authentication mode is specified, that is, the user is unable to log into the system.

You must specify an authentication mode for a new user, otherwise, the user will be unable to log into to the system. The authentication mode set for the new user will take effect the next time when the user log into the system.

For related command, see display ssh user-information.

Example

Set the authentication mode to password for the user smith.

```
[3Com] ssh user smith authentication-type password
[3Com]
```

Chapter 4 NTP Configuration Commands

4.1 debugging ntp-service

Syntax

debugging ntp-service { **access** | **adjustment** | **authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** | **all** }

undo debugging ntp-service { **access** | **adjustment** | **authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** | **all** }

View

User view

Parameter

access: NTP access control debugging.

adjustment: NTP clock adjustment debugging.

all: All NTP debugging.

authentication: NTP authentication debugging.

event: NTP event debugging.

filter: NTP filter debugging.

packet: NTP packet debugging.

parameter: NTP clock parameters debugging.

refclock: NTP reference clock debugging.

selection: NTP clock selection debugging.

synchronization: NTP clock synchronization debugging.

validity: Remote host validity debugging in NTP.

Description

Using the **debugging ntp-service** command, you can debug all the information of the NTP service. Using the **undo debugging ntp-service** command, you can disable the specified debugging.

By default, debugging of all the information is disabled.

Example

Enable NTP access control debugging.

```
[3Com] debugging ntp-service access
```

4.2 display ntp-service sessions

Syntax

display ntp-service sessions [**verbose**]

View

All views

Parameter

verbose: Specifies to or not display the details of sessions.

Description

Using the **display ntp-service sessions** command, you can display the state information of all the sessions maintained by the NTP service of the local device.

By default, the state information of all the sessions maintained by the NTP service of the local device is displayed.

Without the argument **verbose**, the command will display only the brief information of the all the sessions maintained by the local device.

With the argument **verbose**, the command will display the details of the all the sessions maintained by the local device.

Example

Display the information of the sessions maintained by the NTP service at the local device.

```
[3Com] display ntp-service sessions
      source          refid      st  now  poll reach  delay offset   dis
```

```
**************************************************************
[12345]127.127.1.0   LOCAL(0)   7    26   64     1      0.0    0.0   15.6
   [5]10.110.101.20 0.0.0.0   16    -    64     0      0.0    0.0    0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

4.3 display ntp-service status

Syntax

display ntp-service status

View

All views

Parameter

None

Description

Using the **display ntp-service status** command, you can display the state information of the NTP service.

Example

Display the state information of the NTP service.

```
[3Com] display ntp-service status
clock status: synchronized, stratum: 4, reference clock ID: 131.108.13.57
nominal freq: 250.0000 Hz, actual freq: 249.9990 Hz, precision: 2**19
offset: 7.33 ms, reftime: 00:10:22.438 PDT Mon Jul 5 2003 (AFE2525E.70597B34)
root delay  : 133.36 ms, root disper: 126.28 ms, peer disper: 5.98 ms
```

The following table gives the explanation to the displayed information.

Table 4-1 Description of the state information of the NTP server

Item	Description
synchronized	The local system is synchronized with a remote NTP server or some clock source.
unsynchronized	The local system is not synchronized with any remote NTP server.
stratum	The NTP stratum level at which the local system is operating.
reference	Specify the address of the remote server or ID of the clock source with which the local system has synchronized.
nominal freq	The nominal frequency of the hardware clock maintained by the local system
actual freq	The real frequency of the hardware clock maintained by the local system
precision	Precision of the local system clock
reftime	Reference timestamp
offset	The offset of the local clock relative to the NTP server

Item	Description
root delay	Total roundtrip delay to the master reference source
root disper	The maximum error (dispersion) relative to the master reference source
peer disper	The dispersion of the remote NTP server

4.4 display ntp-service trace

Syntax

display ntp-service trace [*X.X.X.X*]

View

All views

Parameter

X.X.X.X: IP address of the NTP server operating as the reference clock source.

Description

Using the **display ntp-service trace** command, you can display the brief information of the NTP time servers passed for tracing back to the reference clock source from the local device.

This command enables you to set out from the local device, trace along the time synchronization NTP server link back to the reference clock source, and display the brief information of all the NTP servers along the link.

Example

Display the brief information of the NTP time servers passed by when tracing from the local device to the reference clock source.

```
[3Com] display ntp-service trace
server4: stratum 4, offset 0.0019529, synch distance 0.144135
server3: stratum 3, offset 0.0124263, synch distance 0.115784
server2: stratum 2, offset 0.0019298, synch distance 0.011993
server1: stratum 1, offset 0.0019298, synch distance 0.011993 refid  'GPS
Reciever'
```

The information shows the synchronization link of server4, along which, server4 synchronizes with server3, server3 with server2, server2 with server1, and server1 with the clock source GRP Reciever.

4.5 ntp-service access

Syntax

ntp-service access { **query** | **synchronization** | **server** | **peer** } *acl-number*

undo ntp-service access { **query** | **synchronization** | **server** | **peer** }

View

System view

Parameter

query: Assigns the controlled query right.

synchronization: Allows only the server to access.

server: Allows the server and query to access.

peer: Full access right.

acl-number: IP ACL number. The basic ACL can be numbered in the range of 1 to 99.

Description

Using the **ntp-service access** command, you can control the access to the service provided by the local device. Using the **undo ntp-service access** command, you can remove the configured access rights.

By default, there is no access restriction.

This command can be used to control the access to the NTP services of the local device. It just provides a minimum security protection, however. To obtain much reliable security, you must configure authentication. Whenever receiving an access request, the router will perform the match operation to find out the access right assigned to the requestor in the descending order of access rights, i.e., **peer**, **server**, **synchronization**, and **query**. The match found first will be the service access right assigned to the requestor.

Example

Assign the **peer** access right to the peers in ACL 76.

```
[3Com] ntp-service access peer 76
```

Assign the **synchronization** access right to the peers in ACL 28.

```
[3Com] ntp-service access synchronization 28
```

4.6 ntp-service authentication enable

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

View

System view

Parameter

None

Description

Using the **ntp-service authentication enable** command, you can enable authentication of NTP services. Using the **undo ntp-service authentication enable** command, you can disable authentication.

By default, authentication is disabled.

Example

Enable NTP authentication.

```
[3Com] ntp-service authentication enable
```

4.7 ntp-service authentication-keyid

Syntax

ntp-service authentication-keyid *number* **authentication-mode md5** *value*

undo ntp-service authentication-keyid *number*

View

System view

Parameter

number: Key number in the range of 1 to 4294967295.

value: Key information, which contains 1 to 32 ASII characters.

Description

Using the **ntp-service authentication-keyid** command, you can set an NTP authentication key. Using the **undo ntp-service authentication-keyid** command, you can remove the NTP authentication key.

By default, there is no authentication key.

This command enables you to set an NTP authentication key. So far, only MD5 authentication is supported.

Example

Set an MD5 authentication key, given the key ID is 10 and the key value is BetterKey.

```
[3Com] ntp-service authentication-keyid 10 authentication-mode md5 BetterKey
```

4.8 ntp-service broadcast-client

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

View

Interface view

Parameter

None

Description

Using the **ntp-service broadcast-client** command, you can configure the NTP broadcast client mode. Using the **undo ntp-service broadcast-client** command, you can disable the NTP broadcast client mode.

By default, NTP broadcast client service is not configured.

With this command, you can specify the current interface on the local device to receive NTP broadcast messages and the local device to work in broadcast-client mode. The local router first detects the broadcast message packets from the server. Upon the receipt of the first broadcast message packet, the local router enters a temporary Client/Server mode to exchange the message with the remote server for the purpose of estimating the network delay, and then it switches to the broadcast

client mode to assume the work of detecting the incoming broadcast message packets with which it can synchronize the local clock.

Example

Receive NTP broadcast messages on the interface Ethernet 1.

```
[3Com] interface Ethernet 1
[3Com-Ethernet1] ntp-service broadcast-client
```

4.9 ntp-service broadcast-server

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

View

Interface view

Parameter

authentication-keyid: Defines a key for authentication.

keyid: The key ID used when sending messages to a broadcast client, which is in the range of 1 to 4294967295.

version: Defines the NTP version number.

number: NTP version number in the range of 1 to 3.

Description

Using the **ntp-service broadcast-server** command, you can enable the NTP broadcast server mode. Using the **undo ntp-service broadcast-server** command, you can disable the NTP broadcast server mode.

By default, the broadcast service is not configured and the version *number* is 3.

You can specify an interface on the local device to send NTP broadcast messages. After that, the local working in broadcast server mode will work as a broadcast server to periodically send broadcast messages to the broadcast clients.

Example

Specify Ethernet 0 for sending NTP broadcast messages, given the key is Key 4 and NTP version is 3.

```
[3Com] interface Ethernet 0
[3Com-Ethernet0] ntp-service broadcast-server authentication-key 4 version 3
```

4.10 ntp-service max-dynamic-sessions

Syntax

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

View

System view

Parameter

number: The number of sessions allowed at the local, which is in the range of 0 to 128.

Description

Using the **ntp-service max-dynamic-sessions** command, you can set the number of sessions allowed at the local. Using the **undo ntp-service max-dynamic-sessions** command, you can restore the default number of sessions allowed at the local.

The maximum number of sessions defaults to 100.

Example

Set the maximum number of sessions allowed at the local to 50.

```
[3Com] ntp-service max-dynamic-sessions 50
```

4.11 ntp-service multicast-client

Syntax

ntp-service multicast-client [*X.X.X.X*]

undo ntp-service multicast-client [*X.X.X.X*]

View

Interface view

Parameter

X.X.X.X: Multicast IP address, that is, Class D address.

Description

Using the **ntp-service multicast-client** command, you can enable the NTP multicast client mode. Using the **undo ntp-service multicast-client** command, you can disable the NTP multicast client mode.

By default, multicast client service is not configured and *X.X.X.X* is 224.0.1.1.

With this command, you can specify the current interface on the local device to receive NTP multicast messages and the local device to work in multicast-client mode. The local router first detects the multicast message packets from the server. Upon the receipt of the first broadcast message packet, the local router enters a temporary Client/Server mode to exchange the message with the remote server for the purpose of estimating the network delay, and then it switches to the broadcast client mode to assume the work of detecting the incoming multicast message packets with which it can synchronize the local clock.

Example

Receive NTP multicast messages on the interface Ethernet 0, given the multicast group address associated to the multicast messages is 224.0.1.1.

```
[3Com] interface Ethernet 0
[3Com-Ethernet0] ntp-service multicast-client 224.0.1.1
```

4.12 ntp-service multicast-server

Syntax

ntp-service multicast-server [*X.X.X.X*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* **| version** *number*] *

undo ntp-service multicast-server [*X.X.X.X*]

View

Interface view

Parameter

X.X.X.X: Class D multicast IP address, which defaults to 224.0.1.1.

authentication-keyid: Defines an authentication key.

keyid: The key ID carried in the messages transmitted to the multicast clients, which is in the range of 1 to 4294967295.

ttl: Defines the Time-To-Live (TTL) period of multicast packets.

ttl-number: The TTL period of multicast packets, which is in the range of 1 to 255.

version: Defines an NTP version.

number: NTP version number in the range of 1 to 3.

Description

Using the **ntp-service multicast-server** command, you can enable the NTP multicast server mode. Using the **undo ntp-service multicast-server** command, you can disable the NTP multicast server mode.

By default, no multicast service is configured, IP address is 224.0.1.1, and the version number is 3.

With this command, you can specify an interface on the local device for sending NTP multicast messages while the local device is running in multicast server mode to periodically send multicast messages to its multicast clients.

Example

Enable the interface Ethernet 0 to send NTP multicast messages, given the multicast group address is 224.0.1.1, key 4 is used for encryption, and NTP version number is 3.

```
[3Com] interface Ethernet 0
[3Com-Ethernet0] ntp-service multicast-server 224.0.1.1 authentication-keyid
4 version 3
```

4.13 ntp-service refclock-master

Syntax

ntp-service refclock-master [*X.X.X.X*] [*stratum*]

undo ntp-service refclock-master [*X.X.X.X*]

View

System view

Parameter

X.X.X.X: IP address of the reference clock, which is in the form of 127.127.t.u.

stratum: The stratum level at which the local clock operates, which is in the range of 1 to 15.

Description

Using the **ntp-service refclock-master** command, you can set an external reference clock or the local clock to be the NTP master clock. Using the **undo ntp-service refclock-master** command, you can remove the settings of NTP master clock.

X.X.X.X is not specified, and *stratum* is 1.

This command can set an external reference clock or local clock as the NTP master clock providing reference for time synchronization of other devices. *X.X.X.X* represents the IP address, that is, 127.127.t.u, of the reference clock. If it has not been specified, the local clock works as the NTP master clock by default. With this command, you can specify the stratum level where the NTP master clock operates.

Example

Set the local device to be the NTP master clock at stratum 3, which provides reference for the time synchronization of other peers.

```
[3Com] ntp-service refclock-master 3
```

4.14 ntp-service reliable authentication-keyid

Syntax

ntp-service reliable authentication-keyid *number*

undo ntp-service reliable authentication-keyid *number*

View

System view

Parameter

number: Key number in the range of 1 to 4294967295.

Description

Using the **ntp-service reliable authentication-keyid** command, you can specify a key to be reliable. Using the **undo ntp-service reliable authentication-keyid** command, you can remove the current setting.

By default, no reliable authentication key is set.

In the event that authentication has been enabled, this command can be used for specifying one or more keys to be reliable. In other words, clients will only synchronize its clock to the server providing a reliable key. Otherwise, clients will refuse synchronization.

Example

Enable NTP authentication, adopt MD5 encryption, set key ID to 37, configure the key as BetterKey and specify the key to be reliable.

```
[3Com] ntp-service authentication enable
[3Com] ntp-service authentication-keyid 37 authentication-mode md5 BetterKey
[3Com] ntp-service reliable authentication-keyid 37
```

4.15 ntp-service source-interface

Syntax

ntp-service source-interface { *interface-name* | *interface-type interface-number* }

undo ntp-service source-interface

View

System view

Parameter

interface-name: Interface name. The IP address of the interface will be used as the source IP address of the messages.

interface-type: Interface type, which identifies an interface along with *interface-number*.

interface-number: Interface number, which identifies an interface along with *interface-type*.

Description

Using the **ntp-service source-interface** command, you can specify a local interface for NTP message transmission. Using the **undo ntp-service source-interface** command, you can remove the current setting.

Source address will be determined depending on the output interface.

Using this command, you can specify a source IP address to be carried by all the transmitted NTP messages by specifying the interface. This command is useful in the case that you do not want the IP addresses of any other local interfaces to be the

destination addresses for receiving the response messages except for the specified one.

Example

Specify the interface Ethernet 0 so that its IP address can be used as the source IP address carried by all the outbound NTP message packets.

```
[3Com] ntp-service source-interface Ethernet 0
```

4.16 ntp-service source-interface disable

Syntax

ntp-service source-interface disable

undo ntp-service source-interface disable

View

Interface view

Parameter

None

Description

Using the **ntp-service source-interface disable** command, you can disable an interface to receive NTP messages. Using the **undo ntp-service source-interface disable** command, you can enable the interface to receive NTP messages.

By default, an interface is enables to receive NTP messages.

Example

Disable Ethernet 0 to receive NTP messages.

```
[3Com] interface Ethernet 0
[3Com-Ethernet0] ntp-service source-interface disable
```

4.17 ntp-service unicast-peer

Syntax

ntp-service unicast-peer *X.X.X.X* [**version** *number* | **authentication-key** *keyid* | **source-interface** { *interface-name* | *interface-type interface-number* } | **priority**] *

undo ntp-service unicast-peer *X.X.X.X*

View

System view

Parameter

X.X.X.X: IP address of the remote server.

version: Defines NTP version number.

number: NTP version number in the range of 1 to 3.

authentication-keyid: Defines an authentication key.

keyid: The key ID carried in the messages transmitted to the remote server, which is in the range of 1 to 4294967295.

source-interface: Specifies interface name.

interface-name: Interface name. The IP address of the interface will be used as the source IP address of the NTP messages that the local device sends to its peer.

interface-type: Interface type, which identifies an interface along with *interface-number*.

interface-number: Interface number, which identifies an interface along with *interface-type*.

priority: Specifies the server to be the preferred server.

Description

Using the **ntp-service unicast-peer** command, you can enable the NTP unicast peer mode. Using the **undo ntp-service unicast-peer** command, you can disable the NTP unicast peer mode.

By default, version *number* is 3, authentication is disabled, and the server is not the preferred choice.

This command sets the remote server at *X.X.X.X* to be the peer of the local device running in symmetric active mode. *X.X.X.X* represents a host address, which must not be a broadcast or multicast address, or the IP address of the reference clock. With all these configurations, the local device can synchronize its clock to the remote server and vice versa.

Example

Set the peer at 128.108.22.44 to be the synchronization source of the local device, allowing the remote peer to synchronize with the local clock. In addition, version 3 is adopted, and IP address of Ethernet 0 is used as the IP source address carried by the NTP messages.

```
[3Com] ntp-service unicast-peer 128.108.22.44 version 3 source-interface
Ethernet 0
```

4.18 ntp-service unicast-server

Syntax

ntp-service unicast-server *X.X.X.X* [**version** *number* | **authentication-keyid** *keyid* | **source-interface** { *interface-name* | *interface-type interface-number* } | **priority**] *

undo ntp-service unicast-server *X.X.X.X*

View

System view

Parameter

X.X.X.X: IP address of the remote server.

version: Defines NTP version.

number: NTP version number in the range of 1 to 3.

authentication-keyid: Defines authentication key ID.

keyed: The key ID should be carried in the messages sent to the remote server, which is in the range of 1 to 4294967295.

source-interface: Specifies the interface name.

interface-name: Interface name. The IP address of the interface will be used as the source IP address of the NTP messages that the local device sends to the defined server.

interface-type: Interface type, which identifies an interface along with *interface-number*.

interface-number: Interface number, which identifies an interface along with *interface-type*.

priority: Specifies the server to be the preferred server.

Description

Using the **ntp-service unicast-server** command, you can enable the NTP server mode. Using the **undo ntp-service unicast-server** command, you can disable the NTP server mode.

By default, version *number* is 3, authentication is enabled, and the server is not the preferred choice.

This command declares that the local time server is the remote server specified by *X.X.X.X*. *X.X.X.X* represents a host address, which must not be a broadcast or multicast address, or the IP address of the reference clock. Configured with this command, the local device is working in client mode and therefore it is up to the local client to synchronize with the remote server rather than vice versa.

Example

Configure the local device to synchronize with the server at 128.108.22.44 and set the version number to 3.

```
[3Com] ntp-service unicast-server 128.108.22.44 version 3
```

Chapter 5 X2T Configuration Commands

5.1 debugging x25 x2t

Syntax

debugging x25 x2t { **all** | **event** | **packet** }

View

All views

Parameter

all: Enables all X2T debugging.

event: Enables the X2T event debugging.

packet: Enables the X2T packet debugging.

Description

Using the **debugging x25 x2t** command, you can enable X2T debugging.

Example

Enable the X2T event debugging.

```
[Router] debugging x25 x2t event
```

5.2 display x25 x2t route

Syntax

display x25 x2t route

View

All views

Parameter

None

Description

Using the **display x25 x2t route** command, you can display the X2T static routing table.

Example

Display the X2T static routing table maintained by the router.

```
[Router]display x25 x2t route
  SID      X.121          Ip Address
==============================================
  1        12321          10.110.54.18
```

5.3 display x25 x2t switch-table

Syntax

display x25 x2t switch-table

View

All views

Parameter

None

Description

Using the **display x25 x2t switch-table** command, you can display the X2T dynamic route switching table.

Example

Display the X2T dynamic route switching table.

```
[Router]display x25 x2t switch-table
  X.121         Interface [LCD]  <--> Ip Address     SocketId
================================================================
```

5.4 translate ip

Syntax

translate ip *ip-address* **port** *port-number* **x25** *x.121-address*

undo translate ip *ip-address* **port** *port-number*

View

System view

Parameter

ip-address: Local IP address.

port *port-number*: TCP port number.

x25 *x.121-address*: The destination X.121 address after the address translation.

Description

Using the **translate ip** command, you can configure an X2T forwarding route from an IP network to an X.25 network. Using the **undo translate ip** command, you can disable the configuration that has been made.

Whenever an IP host sends packets to the specified IP address and port of the router, the router will translate the IP packets into X.25 packets upon the receipt and forward them to the X.121 address on the X.25 network.

Example

Configure an X2T forwarding route for forwarding the packets that the local device receives at 10.110.54.18:102 to the X.121 address 12321.

```
[Router]translate ip 10.110.54.18 port 102 x25 12321
```

5.5 translate x25

Syntax

translate x25 *x.121-address* **ip** *ip-address* **port** *port-number*

undo translate x25 *x.121-address*

View

System view

Parameter

x25 *x.121-address*: Destination X.121 address.

ip-address: The destination IP address after the translation.

port *port-number*: TCP port number.

Description

Using the **translate x25** command, you can configure an X2T forwarding route from the X.25 network to the IP network. Using the **undo translate x25** command, you can disable the configuration that has been made.

Whenever receiving the X.25 packets destined to a specified X.121 address, the router will convert these X.25 packets into IP packets and forward them to the specified IP address in the IP network.

Example

Configure an X2T forwarding route on the router for forwarding the packets destined to the X.121 address 12322 to the IP address 10.110.54.19:102.

```
[Router]translate x25 12322 ip 10.110.54.19 port 102
```

Chapter 6 Additional ISDN Configuration Commands

6.1 isdn ignore callednum

Syntax

isdn ignore callednum

undo isdn ignore callednum

View

ISDN BRI interface view, CE1/PRI interface view, CT1/PRI interface view

Parameter

None

Description

Using the **isdn ignore callednum** command, the user can disable the SETUP ACK messages if the received SETUP messages in data service calls do not carry the called number information.. Using **undo isdn ignore callednum** command, the router will send SETUP ACK messages.

By default, the router that is interoperating with an exchange sends SETUP ACK messages even if the received SETUP messages do not carry the called number information.

The switches of some vendors neither carry the called number information in the SETUP messages nor recognize SETUP ACK messages. In this case, a router must be disabled to send SETUP ACK messages by using this command when interoperating with the switches of such vendors.

With CE1/PRI or CT1/PRI interfaces, you must configure PRI bundling before you can configure this command in serial interface view. For more information about PRI bundling, refer to the commands **pri-set** (CE1/PRI Interface) and **pri-set** (CT1/PRI Interface).

Example

Disable the E1 0 interface on the router to send SETUP ACK messages.

```
[3Com] controller e1 0
[3Com-E1-0] pri-set
[3Com-E1-0] interface serial 2:15
[3Com-serial2:15] isdn ignore callednum
```

6.2 isdn ignore hlc

Syntax

isdn ignore hlc

undo isdn ignore hlc

View

ISDN interface view

Parameter

None

Description

Using the **isdn ignore hlc** command, the user can configure the SETUP message to ignore the high-level compatibility information unit when a data call is initiated. Using the **undo isdn ignore hlc** command**,** you can enable the high-level compatibility information unit in the SETUP message.

By default, the SETUP message carries high-level compatible information unit when the ISDN originates data calls.

When connecting to a European ISDN network, it is necessary to configure this command.

For the related commands, see **isdn ignore llc.**

Example

When connecting to a European ISDN network, if the European network cannot recognize the high-level compatible information unit, it is necessary to configure this command as follows.

```
[3Com-Bri0]isdn ignore hlc
```

6.3 isdn ignore llc

Syntax

isdn ignore llc

undo isdn ignore llc

View

ISDN interface view

Parameter

None

Description

Using the **isdn ignore llc** command, the user can configure the SETUP message to ignore the low-level compatibility information unit when a data call is initiated. Using the **undo isdn ignore llc** command**,** you can enable the low-level compatibility information unit in the SETUP message.

By default, the SETUP message carries low-level compatible information unit when the ISDN originates data calls.

When connecting to a European ISDN network, it is necessary to configure this command.

For related commands, see **isdn ignore hlc.**

Example

When connecting to a European ISDN network, if the European network cannot recognize the low-level compatible information unit, it is necessary to configure this command as follows.

```
[3Com-Bri0]isdn ignore llc
```

6.4 isdn waitconnectack

Syntax

isdn waitconnectack

undo isdn waitconnectack

View

ISDN BRI interface view, CE1/PRI interface view, CT1/PRI interface view

Parameter

None

Description

Using **isdn waitconnectack** command, the user can configure the router to wait for CONNECT ACK message replies from the connected exchange until switching to the ACTIVE state. Using **undo isdn waitconnectack** command, the user can configure the router to become ACTIVE to start data exchange before receiving CONNECT ACK messages. By default, Q.931/Q.SIG must wait for the CONNECT ACK messages before it can be ACTIVE.

Some exchanges will send CONNECT ACK messages but some will not.

Example

Configure the router to become ACTIVE to start data exchange before receiving CONNECT ACK messages.

```
[3Com] undo isdn waitconnectack
```

6.5 display isdn spid

Syntax

display isdn spid [interface *type number*]

View

All views

Parameter

interface type number

Description

Using the **display isdn spid** command, you can view the SPID information on the BRI interface running the NI protocol.

You may execute this command to view the SPID type and SPID value when ISDN is running. Executing this command, without specifying an interface, to view the related

information of SPI on all the SPID-supported BRI interfaces. You may view one interface by specifying its type and number.

Example

Display the related information of SPID on the NI-supported interface bri 0/0/0.

```
[3Com] display isdn spid interface bri 0
Interface bri 0/0/0:
   SPID Type: AUTO
   SPID  B1:
SPID Num 124345

Neg State SPID_ASSIGNED
Init State INIT_NULL
   SPID  B2:
SPID Num 45645754
Neg State SPID_ASSIGNED
Init State INIT_NULL
   SPID timer: 30 seconds
   SPID resend: 2
```

Table 6-1 Description of the SPID parameters

Item	Description
SPID Type	SPID Type, which can be NIT, STATIC (having only the L3 initialization process), or AUTO (including both the negotiation and the L3 initialization).
SPID B1	SPID value of the BRI interface B1 channel. It can be a static configuration or the result of a dynamic negotiation, all depending on the specified SPID Type.
SPID Num	SPID value of the BRI interface. It can be a static configuration or the result of a dynamic negotiation, depending on the specified SPID Type.
Neg State	Negotiation state of the SPID, which can be SPID_UNASSIGNED, ASSIGN_AWAITING_SPID, SPID_ASSIGNED, ASSIGN_AWAITING_CALL_CLEAR.
Init State	Initialization state of the SPID, which can be INIT_NULL, INIT_IND, INIT_PROCEEDING, INIT_END, INIT_AWAITING_CALL_CLEAR.
SPID B2	SPID value of the BRI interface B2 channel. It can be a static configuration or the result of a dynamic negotiation, depending on the specified SPID Type.
SPID timer	Duration of the timer TSPID
SPID resend	SPID message retransmission times

6.6 isdn ignore dchan

Syntax

Isdn ignore dchan

undo Isdn ignore dchan

View

ISDN PRI interface view

Parameter

None

Description

Using the **isdn ignore dchan** command, you can configure the ISDN protocol to use consecutive numbering of B channels during call initiation. 1 will be subtracted from all channel numbers after slot 17, to keep the continuity of the channel serial number. Channels are allocated from 1 to 30.

Use the **undo Isdn ignore dchan** command to return to the default.

🕮 **Note:**

When a router interoperates with an ISDN switch, its configuration should be consistent with that of the switch.

If there is a call on the ISDN interface, you cannot configure this command. Shutdown the ISDN interface manually to configure this command, and then undo shutdown.

Example

Set the ISDN protocol to use consecutive numbering of B channels when a call is originated on PRI interface 0.

```
[3Com-serial0:15] isdn ignore dchan
```

6.7 isdn protocol-type

Syntax

isdn protocol-type { dss1 | ni }

View

System view

Interface view

Parameter

dss1: DSS1 (Digital Subscriber Signaling No.1) signaling is used.

ni: National ISDN signaling is used.

Description

Using the **isdn protocol-type** command, you can configure signaling to be used at the ISDN interface.

By default, DSS1 signaling is used.

When this command is used in System view, it will set the default signaling for the ISDN interface configured on a router, but it will not affect the type of signaling on an existing ISDN interface.

When this command is used in Interface view, it will set the type of signaling for the active ISDN interface. However, if there are calls on the interface, configuring this command will not take effect.

🕮 **Note:**

You are allowed to configure:
DSS1 ISDN on BRI, E1 PRI, and T1 PRI interfaces;
NI (National ISDN) on BRI interfaces;
Other protocols are made up by the negotiation commands of Layer 3 protocol under DSS1 protocol.

For related commands, see **display isdn call-info**.

Example

Configure the router to use NI signaling at the interface BRI0.

```
[3Com-Bri0]isdn protocol-type ni
```

6.8 isdn q931-timer

Syntax

isdn q931-timer timer-name time-interval

undo isdn q931-timer { timer-name | **all** }

View

Interface view

Parameter

timer-name: Name of Q931 timer. Refer to the following table for a description in detail.

time-interval: Interval of timer. Refer to the following table for a description in detail.

all: To be used to restore the default interval values of all the Q931 timers.

Description

Using the **isdn q931-timer** command, you can configure the interval for a Q931 signaling timer. Using the **undo isdn q931-timer** command, you can restore the default interval values of Q931 signaling timers.

Different timers have different default values. Refer to the following table for a description in detail.

Table 6-2 Description of Q931 timers

timer-name	Timer	Value range (in seconds)	Default value (in seconds)
t301	T301	30–1200	180
t302	T302	5–60	15
t303	T303	2–10	5
t304	T304	10–60	30
t305	T305	4–30	30
t308	T308	2–10	5
t309	T309	10–180	90
t310	T310	10–180	30
t313	T313	2–10	5
t316	T316	20–180	120
t322	T322	2–10	4

Example

Set the timer T322 to 6 seconds.

```
[3Com-Serial2:15]isdn q931-timer t322 6
```

6.9 isdn spid auto-trigger

Syntax

isdn spid auto-trigger

View

ISDN BRI Interface view

Parameter

None

Description

Using the **isdn spid auto-trigger** command, you can enable SPID auto-negotiation once on the BRI interface running the NI protocol.

On a BRI interface compliant with the North American ISDN protocol, the router can place a call only after SPID negotiation or initialization. SPID information can be obtained via static configuration or dynamic negotiation. You may manually trigger a new SPID negotiation request by executing this command if the SPID negotiation in dynamic negotiation fails or just for the purpose of testing.

By default, a BRI interface does not originate a SPID negotiation request unless triggered by a call.

This command applies only on the BRI interface running the NI protocol.

Example

Manually trigger a new SPID negotiation request on the interface bri0.

```
[3Com-bri0] isdn spid auto-trigger
```

6.10 isdn spid nit

Syntax

isdn spid nit

undo isdn spid nit

View

ISDN BRI Interface view

Parameter

None

Description

Using the **isdn spid nit** command, you can set the SPID processing mode to NIT (Not Initial Terminal) on an NI-compliant BRI interface. Using the **undo isdn spid nit** command, you can disable the NIT mode on the BRI interface.

By default, NIT mode does not apply on BRI interfaces. Instead, static SPID or dynamic SPID negotiation is applied.

On an NI-compliant BRI interface, calls can be placed only after the SPID negotiation or initialization is finished. When the router is communicating with an NI-compliant exchange that does not support SPID negotiation, you can use this command to set the SPID processing mode on the router to NIT and ISDN will ignore ISPID negotiation and initialization.

This command applies only on NI-compliant BRI interfaces.

Example

Ignore SPID negotiation and initialization on interface bri0.

```
[3Com-bri0] isdn spid nit
```

6.11 isdn spid timer

Syntax

isdn spid timer *seconds*

undo isdn spid timer

View

ISDN BRI Interface view

Parameter

seconds: Duration of the SPID timer, which is in the range of 1 to 255 seconds, and defaults to 30 seconds.

Description

Using the **isdn spid timer** command, you can set the duration of the timer TSPID for an NI-compliant BRI interface to timer length. Using the **undo isdn spid timer** command, you can restore the default duration of the timer TSPID for the NI-compliant BRI interface.

On a BRI interface compliant with the ISDN protocol in North America, calls can be placed only after the SPID negotiation or initialization is finished. SPID information can be obtained via static configuration or dynamic negotiation. The timer TSPID is started when the terminal originates a negotiation or initialization request by sending the INFORMATION message. You can use this command to modify the duration of TSPID.

This command applies only on NI-compliant BRI interfaces.

Example

Set the duration of TSPID on the interface bri0 to 50 seconds.

```
[3Com-bri0] isdn spid timer 50
```

6.12 isdn spid resend

Syntax

isdn spid resend *times*

undo isdn spid resend

View

ISDN BRI Interface view

Parameter

times: An integer in the range of 1 to 255 times, which defaults to 1.

Description

Using the **isdn spid resend** command, you can set the number of INFORMATION message retransmission attempts for SPID negotiation or initialization on an NI-compliant BRI interface. Using the **undo isdn spid resend** command, you can restore the default number of INFORMATION message retransmission attempts on the interface.

On a BRI interface compliant with the ISDN protocol in North America, calls can be placed only after the SPID negotiation or initialization is finished. The timer TSPID is started when the terminal originates a negotiation or initialization request by sending the INFORMATION message. If the terminal does not receive any response upon the expiration of TSPID, it will retransmit the INFORMAITON message. You can use this command to modify the number of INFORMATION message retransmission attempts.

This command applies only on NI-compliant BRI interfaces.

Example

Set the allowed number of INFORMATION retransmission attempts to five.

```
[3Com-bri0] isdn spid resend 5
```

6.13 isdn spid service

Syntax

isdn spid service [audio | data | speech]

undo isdn spid service

View

ISDN BRI interface view

Parameter

audio: Supports audio service.

data: Supports data service.

speech: Supports voice service.

Description

Using the **isdn spid service** command, you can configure the service types that must be supported in SPI negotiation on the BRI interface using NI protocol. Using the **undo isdn spid service** command, you can delete the service types that must be supported in SPI negotiation on the BRI interface using NI protocol.

There are three types of services. You can select any one or none. None means all services are supported. By default, SPID supports data and voice service simultaneously.

For BRI interfaces using National ISDN protocol, you need to negotiate or initialize a SPID before originating a call. During negotiation, SPCS may send multiple SPIDs, and carry the service types supported by the SPID, so the router needs to choose a proper SPID according to the local service type.

This command can only be applied on the BRI interface using NI protocol.

Example

Set the service type supported by the BRI interface to data and voice.

```
[3Com-bri0] isdn spid service data
[3Com-bri0/0] isdn spid service speech
```

6.14 isdn spid1

Syntax

isdn spid1 *spid*

undo isdn spid1

View

ISDN BRI Interface view

Parameter

spid: String comprising 9 to 20 digits.

Description

Using the **isdn spid1** command, you can configure SPID information for the B1 channel on an NI-compliant BRI interface. Using the **undo isdn spid1** command, you can remove the SPID information form the B1 channel on the interface.

On a BRI interface compliant with the ISDN protocol in North America, calls can be placed only after the SPID negotiation or initialization is finished. SPID information can be obtained via static configuration or dynamic negotiation. Only after SPID information is configured for the B1 channel on the BRI interface can the system make the L3 initialization to place calls.

By default, SPID for the B1 channel on a BRI interface is null.

This command applies only on NI-compliant BRI interfaces.

Example

Set SPID to “012345” for the B1 channel on the interface bri0.

```
[3Com-bri0] isdn spid1 012345
```

6.15 isdn spid2

Syntax

isdn spid2 *spid*

undo isdn spid2

View

ISDN BRI Interface view

Parameter

spid: String comprising 9 to 20 digits.

Description

Using the **isdn spid2** command, you can configure SPID information for the B1 channel on an NI-compliant BRI interface. Using the **undo isdn spid2** command, you can remove the SPID information from the B1 channel on the interface.

On a BRI interface compliant with the ISDN protocol in North America, calls can be placed only after the SPID negotiation or initialization is finished. SPID information can be obtained via static configuration or dynamic negotiation. Only after SPID information is configured for the B1 channel on the BRI interface can the system make the L3 initialization to place calls.

By default, SPID for the B2 channel on a BRI interface is null.

This command applies only on NI-compliant BRI interfaces.

Example

Set SPID to “012345” for the B2 channel on the interface bri0.

```
[3Com-bri0] isdn spid2 012345
```